

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-214297

(43)Date of publication of application : 11.08.1998

(51)Int.CI.

G06F 17/60  
G06F 13/00  
G06F 13/00  
G06F 15/00

(21)Application number : 09-323626

(22)Date of filing : 25.11.1997

(71)Applicant : FUJITSU LTD

(72)Inventor : OKI HIROSHI  
KAMATA SHINJI  
NAKAMURA NAOTO  
YAMAZAKI TOSHIYA  
OKADA TOSHIO

(30)Priority

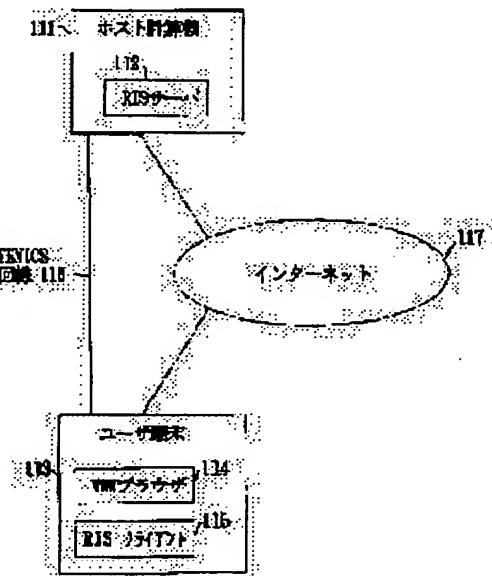
Priority number : 08318113 Priority date : 28.11.1996 Priority country : JP

## (54) CLOSED-MEMBERSHIP SERVICE SYSTEM USING INTERNET, AND METHOD THEREFOR

## (57)Abstract:

**PROBLEM TO BE SOLVED:** To execute a safe and proper closed-membership service by using a remote install system on an internet.

**SOLUTION:** A remote install service(RIS) client 115 activated by a WWW browser 114 communicates a software number corresponding to an icon clicked on a home page to an RIS server 112. The RIS server 112 provides each kind of service such as software delivery, on-line shopping, communication service, and transaction service based on the information. A password or a content is enciphered and transferred on an internet 117.



## LEGAL STATUS

[Date of request for examination] 21.09.2000

[Date of sending the examiner's decision of rejection] 06.01.2004

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection] 2004-02170

[Date of requesting appeal against examiner's decision of rejection] 05.02.2004

[Date of extinction of right]

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平10-214297

(43)公開日 平成10年(1998)8月11日

(51)Int.Cl. <sup>8</sup>	識別記号	F I	
G 06 F 17/60		G 06 F 15/21	3 3 0
13/00	3 5 1	13/00	3 5 1 H
	3 5 7		3 5 7 Z
15/00	3 3 0	15/00	3 3 0 Z

審査請求 未請求 請求項の数49 O.L (全 56 頁)

(21)出願番号 特願平9-323626  
(22)出願日 平成9年(1997)11月25日  
(31)優先権主張番号 特願平8-318113  
(32)優先日 平8(1996)11月28日  
(33)優先権主張国 日本 (JP)

(71)出願人 000005223  
富士通株式会社  
神奈川県川崎市中原区上小田中4丁目1番  
1号  
(72)発明者 沖 宏志  
神奈川県川崎市中原区上小田中4丁目1番  
1号 富士通株式会社内  
(72)発明者 鎌田 紳二  
神奈川県川崎市中原区上小田中4丁目1番  
1号 富士通株式会社内  
(74)代理人 弁理士 大菅 義之 (外1名)

最終頁に続く

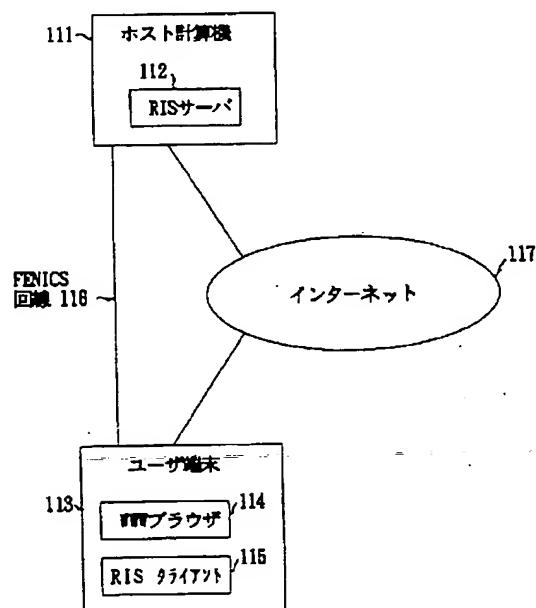
(54)【発明の名称】 インターネットを利用した会員制サービスシステムおよび方法

(57)【要約】

【課題】 インターネット上でリモートインストールシステムを利用して、安全かつ適切な会員制サービスを実現することが課題である。

【解決手段】 WWWブラウザ114により起動されたリモートインストールサービス(RIS)クライアント115は、ホームページ上でクリックされたアイコンに対応するソフトウェア番号を、RISサーバ112に通知する。RISサーバ112は、その情報を元にして、ソフトウェア配達、オンラインショッピング、通信サービス、トランザクションサービス等の各種サービスを提供する。インターネット117上で、パスワードやコンテンツは暗号化されてやり取りされる。

シス テ ム 構 成 図



## 【特許請求の範囲】

【請求項1】 セキュリティの確保された通信路を介して、クライアントのサインアップを行う登録手段と、前記サインアップの過程で、前記クライアントのマシン識別子に対応したキー情報を付与するキー情報付与手段と、

前記キー情報を用いて、インターネット上のパスワードとソフトウェアコンテンツのうち少なくとも一方の暗号化を行う暗号化手段とを備えることを特徴とするソフトウェア配送システム。

【請求項2】 ホームページ上のアンカーファイルにより指定されるソフトウェアを、自動的にサーバからクライアントに配達するリモートインストール手段と、前記アンカーファイルがアクセスされたとき、自動的に前記リモートインストール手段を起動するブラウザ手段とを備えることを特徴とするソフトウェア配送システム。

【請求項3】 前記リモートインストール手段は、インターネットブラウザのヘルパ・アプリケーションとして登録され、前記アンカーファイルに対応する前記ホームページ上の領域がクリックされたとき、自動的に起動されることを特徴とする請求項2記載のソフトウェア配送システム。

【請求項4】 自動的にクライアントからサーバへ接続して、ホームページ上のアンカーファイルにより指定される商品またはサービスの課金処理を行う課金手段と、前記アンカーファイルがアクセスされたとき、自動的に前記課金手段を起動するブラウザ手段とを備えることを特徴とするオンラインショッピングシステム。

【請求項5】 前記課金手段は、自動的に前記サーバから前記クライアントへ情報を配達するリモートインストールシステムを含むことを特徴とする請求項4記載のオンラインショッピングシステム。

【請求項6】 前記課金手段は、インターネットブラウザのヘルパ・アプリケーションとして登録され、前記アンカーファイルに対応する前記ホームページ上の領域がクリックされたとき、自動的に起動されることを特徴とする請求項4記載のオンラインショッピングシステム。

【請求項7】 前記課金手段は、前記商品またはサービスのベンダに購入通知を送ることを特徴とする請求項4記載のオンラインショッピングシステム。

【請求項8】 ホームページ上のアンカーファイルにより指定される通信サービスの課金処理を行い、該通信サービスを利用するため必要な情報を、自動的にサーバからクライアントへ送る処理手段と、前記アンカーファイルがアクセスされたとき、自動的に前記処理手段を起動するブラウザ手段とを備えることを特徴とする通信サービスシステム。

【請求項9】 前記処理手段は、自動的に前記サーバから前記クライアントへ情報を配達するリモートインスト

ールシステムを含むことを特徴とする請求項8記載のオンラインショッピングシステム。

【請求項10】 前記処理手段は、インターネットブラウザのヘルパ・アプリケーションとして登録され、前記アンカーファイルに対応する前記ホームページ上の領域がクリックされたとき、自動的に起動されることを特徴とする請求項8記載のオンラインショッピングシステム。

【請求項11】 前記処理手段は、前記必要な情報をしてパスワード情報をユーザーに通知し、該ユーザーは該パスワード情報を前記ブラウザ手段に入力して、前記通信サービスを利用することを特徴とする請求項8記載のオンラインショッピングシステム。

【請求項12】 前記処理手段は、前記必要な情報をして前記通信サービスのURL (uniform resource locator) 情報をユーザーに通知し、該ユーザーは該URL情報を前記ブラウザ手段に入力して、前記通信サービスを利用することを特徴とする請求項8記載のオンラインショッピングシステム。

【請求項13】 ホームページ上のアンカーファイルにより指定される通信サービスの課金処理を行い、該通信サービスのURL (uniform resource locator) を参照するブラウザを自動的に起動する処理手段と、前記アンカーファイルがアクセスされたとき、自動的に前記処理手段を起動するブラウザ手段とを備えることを特徴とする通信サービスシステム。

【請求項14】 インターネットにアクセスするブラウザ手段と、

前記ブラウザ手段により起動され、トランザクションサービスの一部の処理を行うヘルパ手段と、前記ブラウザ手段により起動され、前記ヘルパ手段と連携して、トランザクションの使用権の付与および課金に関する処理を行う処理手段とを備えることを特徴とするトランザクションサービスシステム。

【請求項15】 前記処理手段は、自動的に前記サーバから前記クライアントへ情報を配達するリモートインストールシステムを含むことを特徴とする請求項14記載のトランザクションサービスシステム。

【請求項16】 トランザクションサービスの処理を行うトランザクション手段と、

前記トランザクション手段により起動され、該トランザクション手段と連携して、トランザクションの使用権の付与および課金に関する処理を行う処理手段とを備えることを特徴とするトランザクションサービスシステム。

【請求項17】 前記処理手段は、前記トランザクションサービスの複数回の使用権を付与することを特徴とする請求項14または16記載のトランザクションサービスシステム。

【請求項18】 トランザクションサービスの処理を行うトランザクション手段と、

3

前記トランザクション手段により起動され、自動的にクライアントからサーバへ接続して、前記トランザクションサービスに必要なデータを取得する処理手段とを備えることを特徴とするトランザクションサービスシステム。

【請求項19】 前記処理手段は、前回のデータ更新時から所定時間経過したとき、前記サーバに接続し、前記データを取得することを特徴とする請求項18記載のトランザクションサービスシステム。

【請求項20】 クライアントから、サーバ識別子とクライアント識別子を合成して生成されたマシン識別子を受け取る受信手段と、

前記マシン識別子をサーバ部とクライアント部に分解し、該サーバ部に記述されたサーバ識別子をチェックして、前記クライアントとの接続が正しいかどうかを判定する判定手段とを備えることを特徴とするサービスシステム。

【請求項21】 サーバ識別子とクライアント識別子を合成して、クライアントのマシン識別子を生成する生成手段と、

前記マシン識別子を格納する格納手段と、

前記マシン識別子を用いてサーバに接続する接続手段とを備えることを特徴とするサービスシステム。

【請求項22】 前記格納手段は、複数のサーバのマシン識別子を、各サーバ毎に記述した複数の初期設定ファイルを格納し、該複数の初期設定ファイルのうちの1つに、他の初期設定ファイルがあるかどうかを表す拡張情報が記述されることを特徴とする請求項21記載のサービスシステム。

【請求項23】 サーバへのログイン時に、該サーバの認証鍵に基づく電子署名機能を用いて暗号化された指定情報を送受信する通信手段と、

該指定情報を介してサーバの認証を行う認証手段とを備えることを特徴とするリモートインストールシステム。

【請求項24】 前記通信手段は、ログインの度に前記認証鍵を取得することを特徴とする請求項23記載のリモートインストールシステム。

【請求項25】 クライアント側に設けられ、インターネット上におけるサーバのアドレス情報を格納する格納手段と、

前記アドレス情報を用いて、自動的に前記クライアントから前記サーバに接続する接続手段とを備えることを特徴とするリモートインストールシステム。

【請求項26】 セキュリティの確保された通信路を介して、クライアントのサインアップを行い、

前記クライアントのマシン識別子に対応したキー情報を前記クライアントに付与し、

前記キー情報を用いて、インターネット上のパスワードとソフトウェアコンテンツのうち少なくとも一方の暗号化を行うことを特徴とするソフトウェア配送方法。

4

【請求項27】 リモートインストールシステムをブラウザのヘルパとして登録し、

ホームページ上に前記ヘルパを起動するアンカーファイルを置き、

前記アンカーファイルがアクセスされたとき、指定されたソフトウェアを、自動的にサーバからクライアントに配達することを特徴とするソフトウェア配達方法。

【請求項28】 リモートインストールシステムをブラウザのヘルパとして登録し、

10 ホームページ上に前記ヘルパを起動するアンカーファイルを置き、

前記アンカーファイルがアクセスされたとき、自動的にクライアントからサーバへ接続して、指定された商品またはサービスの課金処理を行うことを特徴とするオンラインショッピング方法。

【請求項29】 リモートインストールシステムをブラウザのヘルパとして登録し、

ホームページ上に前記ヘルパを起動するアンカーファイルを置き、

20 前記アンカーファイルがアクセスされたとき、指定された通信サービスの課金処理を行い、該通信サービスを利用するためには必要な情報を、自動的にサーバからクライアントへ送ることを特徴とする通信サービス方法。

【請求項30】 リモートインストールシステムをブラウザのヘルパとして登録し、

ホームページ上に前記ヘルパを起動するアンカーファイルを置き、

前記アンカーファイルがアクセスされたとき、指定された通信サービスの課金処理を行い、該通信サービスのU

30 RL (uniform resource locator) を参照するブラウザを自動的に起動することを特徴とする通信サービス方法。

【請求項31】 トランザクションサービスの一部の処理をブラウザの第1のヘルパとして登録し、

トランザクションの使用権をリモートインストールシステムに登録し、

前記リモートインストールシステムを前記ブラウザの第2のヘルパとして登録し、

前記リモートインストールシステムが前記第1のヘルパ40 と連携して、前記トランザクションの使用権の付与および課金に関する処理を行うことを特徴とするトランザクションサービス方法。

【請求項32】 トランザクションの使用権をリモートインストールシステムに登録し、

トランザクション処理ソフトウェアから前記リモートインストールシステムを起動し、

前記リモートインストールシステムが、前記トランザクション処理ソフトウェアと連携して、前記トランザクションの使用権の付与および課金に関する処理を行うこと

50 を特徴とするトランザクションサービス方法。

5

【請求項33】 トランザクション処理ソフトウェアからリモートインストールシステムを起動し、自動的にクライアントからサーバへ接続して、トランザクションサービスに必要なデータを取得することを特徴とするトランザクションサービス方法。

【請求項34】 サーバ識別子とクライアント識別子を合成してマシン識別子を生成し、クライアントからサーバに送られた前記マシン識別子をサーバ部とクライアント部に分解し、前記サーバ部に記述されたサーバ識別子をチェックして、前記クライアントとの接続が正しいかどうかを判定することを特徴とするサービス方法。

【請求項35】 サーバへのログイン時に、該サーバの認証鍵に基づく電子署名機能を用いて暗号化された指定情報を送受し、該指定情報を介してサーバの認証を行うことを特徴とするリモートインストール方法。

【請求項36】 インターネット上におけるサーバのアドレス情報をクライアントに格納し、前記アドレス情報を用いて、自動的に前記クライアントから前記サーバに接続することを特徴とするリモートインストール方法。

【請求項37】 コンピュータのためのプログラムを記録した記録媒体であって、セキュリティの確保された通信路を介して、クライアントのサインアップを行う機能と、前記クライアントのマシン識別子に対応したキー情報を受信する機能と、前記キー情報を用いて、インターネット上のパスワードを暗号化し、暗号化されたパスワードを送信する機能とを前記コンピュータに実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項38】 コンピュータのためのプログラムを記録した記録媒体であって、セキュリティの確保された通信路を介して、クライアントからのサインアップを受け付ける機能と、前記クライアントのマシン識別子に対応したキー情報を前記クライアントに付与する機能と、前記キー情報を用いて、ソフトウェアコンテンツを暗号化し、暗号化されたソフトウェアコンテンツを前記クライアントに送信する機能とを前記コンピュータに実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項39】 コンピュータのためのプログラムを記録した記録媒体であって、ホームページ上のアンカーファイルにより指定されるソフトウェアを、自動的にサーバからクライアントに配達するリモートインストール機能と、前記アンカーファイルがアクセスされたとき、ブラウザに組み込まれた前記リモートインストール機能を自動的

6

に起動する機能とを前記コンピュータに実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項40】 コンピュータのためのプログラムを記録した記録媒体であって、自動的にクライアントからサーバへ接続して、ホームページ上のアンカーファイルにより指定される商品またはサービスの課金を依頼する処理機能と、前記アンカーファイルがアクセスされたとき、ブラウザに組み込まれた前記処理機能を自動的に起動する機能とを前記コンピュータに実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項41】 コンピュータのためのプログラムを記録した記録媒体であって、ホームページ上のアンカーファイルにより指定される通信サービスの課金をサーバに依頼し、該通信サービスを利用するためには必要な情報を、自動的に該サーバから受信する処理機能と、

前記アンカーファイルがアクセスされたとき、ブラウザに組み込まれた前記処理機能を自動的に起動するブラウザ手段とを前記コンピュータに実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項42】 コンピュータのためのプログラムを記録した記録媒体であって、ホームページ上のアンカーファイルにより指定される通信サービスの課金を依頼し、該通信サービスのURL(uniform resource locator)を参照する第1のブラウザを自動的に起動する処理機能と、

前記アンカーファイルがアクセスされたとき、第2のブラウザに組み込まれた前記処理機能を自動的に起動する機能とを前記コンピュータに実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項43】 コンピュータのためのプログラムを記録した記録媒体であって、インターネットにアクセスするブラウザ機能により起動され、トランザクションサービスの一部の処理を行う処理機能と、

前記ブラウザ機能により起動され、前記処理機能と連携して、トランザクションの使用権の付与および課金に関する処理を行う機能とを前記コンピュータに実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項44】 コンピュータのためのプログラムを記録した記録媒体であって、トランザクションサービスの処理を行うトランザクション機能と、前記トランザクション機能により起動され、該トランザクション機能と連携して、トランザクションの使用権の付与および課金に関する処理を行う機能とを前記コンピュータに実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

ュータ読み取り可能な記録媒体。

【請求項45】コンピュータのためのプログラムを記録した記録媒体であって、  
トランザクションサービスの処理を行うトランザクション機能と、  
前記トランザクション機能により起動され、自動的にクライアントからサーバへ接続して、前記トランザクションサービスに必要なデータを取得する機能とを前記コンピュータに実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項46】コンピュータのためのプログラムを記録した記録媒体であって、  
クライアントから、サーバ識別子とクライアント識別子を合成して生成されたマシン識別子を受信する機能と、  
前記マシン識別子をサーバ部とクライアント部に分解し、該サーバ部に記述されたサーバ識別子をチェックして、前記クライアントとの接続が正しいかどうかを判定する機能とを前記コンピュータに実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項47】コンピュータのためのプログラムを記録した記録媒体であって、  
サーバ識別子とクライアント識別子を合成して、クライアントのマシン識別子を生成する機能と、  
前記マシン識別子を格納する機能と、  
前記マシン識別子を用いてサーバに接続する機能とを前記コンピュータに実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項48】コンピュータのためのプログラムを記録した記録媒体であって、  
サーバへのログイン時に、該サーバの認証鍵に基づく電子署名機能を用いて暗号化された指定情報を送受信する機能と、  
該指定情報を介してサーバの認証を行う機能とを前記コンピュータに実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項49】コンピュータのためのプログラムを記録した記録媒体であって、  
インターネット上におけるサーバのアドレス情報をクライアントに格納する機能と、  
前記アドレス情報を用いて、自動的に前記クライアントから前記サーバに接続する機能とを前記コンピュータに実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

#### 【発明の詳細な説明】

##### 【0001】

【発明の属する技術分野】本発明は、インターネット等の通信ネットワークを利用した会員制のサービスを提供するシステムおよびその方法に関する。

##### 【0002】

【従来の技術】近年のパーソナルコンピュータの普及に伴い、ユーザは通信回線を介して様々なサービスを受けられるようになりつつある。例えば、通信回線を介してソフトウェアの配達を自動的に行う従来の技術として、「リモートインストールシステムおよび方法」(特願平7-1797、特開平8-190472)がある。

【0003】従来のリモートインストールサービスシステム(RISシステム)は、ソフトウェアの配達センターにあるホスト計算機、ユーザ端末、およびこれらを結ぶ通信回線から成る。ホスト計算機は、配達可能な複数のソフトウェアを含むソフトウェア群と、そのソフトウェア群から特定のソフトウェアを選択するときに用いるキーワードのリストを保持する第1キーテーブルおよび第2キーテーブルを格納している。

【0004】ユーザが端末からホスト計算機にキーワードのリストを要求すると、ホスト計算機は第1キーテーブル、第2キーテーブルを順次送信して、それらに含まれるキーワードを端末の表示装置の画面に表示させる。ユーザは表示されたキーワードから希望するソフトウェアに対応するものを選び、ホスト計算機に通知する。

【0005】ホスト計算機は通知されたキーワードに該当するいくつかのソフトウェアの名称を含むメニューを表示装置の画面に表示させ、ユーザはその中から希望するソフトウェアを選んで、ホスト計算機に通知する。そして、ホスト計算機はソフトウェア群からユーザの選んだソフトウェアのコンテンツ(ファイル)を取り出し、端末のハードディスクに設定された配達用のディレクトリに格納する。

【0006】このとき、宅配されたソフトウェアを起動するためのアイコンが自動的に登録され、表示装置の画面上でディレクトリに対応して設けられた倉庫ウィンドウ内に表示される。例えば端末がWINDOWSを搭載している場合は、宅配されたソフトウェアはWINDOWSのプログラムマネージャに登録される。以後、ユーザはそのアイコンをマウス等の入力装置を用いてクリックするだけで、宅配されたソフトウェアを使用することができる。

【0007】ここで、図44から図46までを参照しながら、従来のリモートインストールシステムによるソフトウェアの宅配の動作フローを説明する。図44において、ユーザAの端末は通信用の端末ソフトのインストール時に動作環境の情報を取得し、取得した情報を設定した環境ファイル1を作成する(ステップS1)。このとき、ユーザの端末の機種や宅配に使用する格納場所(ディレクトリ)SOUKO等の、取得に時間のかかる情報、あるいは、場合によってユーザに問い合わせなければならない情報を取得する。

【0008】格納場所SOUKOの決定にあたっては、端末はそのハードディスクに所定の容量以上の空き領域があるかどうかを調べ、空き領域があればそのルートに

宅配用のディレクトリを作成する。このときディレクトリ名等は端末が自動的に生成し、ユーザAはそれを確認する作業のみを行う。したがって、ユーザAはディレクトリ名等を入力する必要がない。

【0009】ここでは、ユーザAの機種はTOWNSであり、SOUKOのディレクトリはD:¥SOUKO(ドライブDのディレクトリSOUKO)であることが環境ファイル1に書き込まれる。ユーザAは、必要があればD:¥SOUKOを他のディレクトリに変更することもできる。

【0010】既に設定されているパーティションに所定の容量の空き領域がなければ、別のパーティションの空き領域が一番大きい場所を探して、そこに宅配用のディレクトリを作成する。具体的には、ディレクトリD:¥SOUKOが一杯になったとすると、端末が”D:¥SOUKOが一杯です。倉庫をF:¥SOUKOに変更します。よろしいですか。”等のメッセージを表示装置の画面に表示する。

【0011】ユーザAがこれを承認すると、F:¥SOUKOが新たにSOUKOのディレクトリとなる。所定の容量の空き領域がどのハードディスクにもなかったときは、”残念ながらディスク容量が足りません。ディスクを増設してください。”等のメッセージが表示される。

【0012】次に、端末ソフトの起動時（ホスト計算機へのアクセス時）に、ハードディスクやメモリの状況等のインストール後に変化した可能性のある情報を取得する（ステップS2）。ここでは、ユーザAのハードディスクがドライブDにあり、空き容量が300Mバイトであることが環境ファイル1に書き込まれる。こうして作成された環境ファイル1の内容は、ユーザAがホスト計算機にアクセス（接続）したときに、コマンドRIS\_SENDENVによりホスト計算機に送信される（ステップS3）。

【0013】ホスト計算機は受信した情報をユーザA環境ファイル2として保持する。ユーザA環境ファイル2には、機種、ハードディスク情報HD、格納場所SOUKOのほかに、使用しているOS（オペレーティングシステム）とその格納場所が記述されている。ここでは、ユーザAの端末のOSはWINDOWSであり、その格納場所WINDIRはD:¥WINDOWSであることわかる。

【0014】ホスト計算機からコマンドRIS\_SENDENVに対するレスポンスとしてRIS\_SENDENV\*RESP OKを受け取ると、端末はコマンドRISKEYLISTにより第1キーリストを要求する（ステップS4）。これに応じて、ホスト計算機21は第1キーテーブル3の内容をRISKEYLIST\*RESPとともに送り返す。ここでは、第1キーテーブル3には、キーパー番号1、2、3、…に対応するキー

ワードとして、OS／基本ソフト、開発支援、ゲーム、…が格納されている。

【0015】これらのキーワードが第1キーリストとして表示装置の画面に表示されると（ステップS5）、ユーザAはそれらの中から第1キーワードを選び端末に入力する（ステップS6）。すると、端末はユーザAの選んだ第1キーワードのキー番号とともに、第2キーリストを要求するコマンドRIS\_KEYLISTをホスト計算機に送る（ステップS7）。ここでは、ユーザAは第1キーワードとしてゲームを選択し、それに対応するキー番号3がホスト計算機に送られる。

【0016】第2キーリストを要求されたホスト計算機は、受け取ったキー番号に対応して第1キーテーブル3内に格納されているポインタを用いて、対応する第2キーテーブル4を求め、その内容をRIS\_KEYLIST\*RESPとともに送り返す。ここでは、第2キーテーブル4には、キー番号51、52、53、…に対応するキーワードとして、RPG、アクション、パズル／クイズ、…が格納されている。

【0017】第2キーテーブル4は第1キーテーブル3内のキーワードに対応して一般に複数設けられており、その数は第1キーテーブル3内のキーワードの数と同じか、またはそれより少ない。後者の場合には、第1キーテーブル3内の2つ以上のキーワードが同じ1つの第2キーテーブル4を指すことになる。

【0018】第2キーテーブル4内のキーワードが第2キーリストとして表示装置の画面に表示されると（ステップS8）、ユーザAはそれらの中から第2キーワードを選び端末に入力する（図45、ステップS9）。すると、端末はユーザAの選んだ第1および第2キーワードのキー番号とともに、第1および第2キーワードの両方に該当するソフトウェアのリストを要求するコマンドRIS\_LISTをホスト計算機に送る（ステップS10）。ここでは、ユーザAは第2キーワードとしてアクションを選択し、それに対応するキー番号52がホスト計算機に送られる。

【0019】ソフトウェアのリストを要求されたホスト計算機は、第1および第2キーワードの2つのキー番号を持つソフトウェアをソフトウェア群の中から検索する。このとき、検索条件として第1キーワードと第2キーワードとを区別せずに、フラットに検索を行う。また、機種やOSの種別はデフォルトのキーとして扱い、これらも加味した上で検索する。これにより、例えばTOWNS以外の機種専用のソフトウェアが検索されてくることが防止される。

【0020】そして、該当するソフトウェアの名称と番号のリストをRIS\_LIST\*RESPとともに端末に送る。ここでは、キー番号3と52を持つテリス、バチンコ等のソフトウェアが該当するので、それらの名称がそれぞれのソフトウェア番号5、30等とともに端

末に送られる。

【0021】ソフトウェアのリストが表示装置の画面に表示されると（ステップS11）、ユーザAはそれらの中から希望するソフトウェアを選び、端末に入力する（ステップS12）。すると、端末はユーザAの選んだソフトウェアの番号とともに、ユーザAの環境がそのソフトウェアの動作に適するかどうかのチェックを要求するコマンドRIS\_CHKENVをホスト計算機に送る（ステップS13）。ここでは、ユーザAはテトリスを選択し、それに対応するソフトウェア番号5がホスト計算機に送られる。

【0022】ユーザAが選択したソフトウェアの番号を受け取ったホスト計算機は、その番号に対応するソフトウェアの動作環境とユーザAの端末の環境との整合性を調べるためにチェックスクリプト5を用意し、環境チェックを行う。

【0023】このチェックはチェックスクリプト5の実行プログラムと端末の端末ソフトとの間のやりとりにより自動的に行われる所以、ユーザAは環境チェックが行われていることを必ずしも意識する必要はない（ステップS14）。ユーザAに何らかの問い合わせを行う必要が生じたときにのみ、ホスト計算機がその問い合わせを行ふ。

【0024】ここでは、ユーザAが選択したテトリスの動作環境として、OSがWINDOWS、機種がTOWNS、PC98等、推奨ディレクトリ（DIR）名がTECTであることが記述されている。これに対して、ユーザA環境ファイル2には、機種がTOWNS、OSがWINDOWSと記述されており、両者を比較することによって機種とOSが適合していることがわかる。

【0025】次に、テトリスのチェックスクリプト5を見るとユーザA側の格納場所WINDIRにVBRJP200.DLLというファイルがあるかどうか調査するためのコマンド”ST4 @WINDIR@VBRJP200.DLL”があるので（MQ1）、ホスト計算機はこれをRIS\_CHKENV\*RESPとともに端末に送る。このとき、ホスト計算機はユーザA環境ファイル2を参照して、@WINDIR@をD:¥WINDOWSに置き換えて送る。また、ファイルVBRJP200.DLLはテトリスの動作に必要なファイルの1つである。

【0026】このコマンドを受け取った端末は、ドライブDのディレクトリWINDOWSにファイルVBRJP200.DLLがあるかどうか調べ、その結果をANSとしてホスト計算機に送り返す。ここでは、該当するファイルがなかったのでANS=OFFが送り返される。

【0027】端末にファイルVBRJP200.DLLがないことを知ったホスト計算機は、チェックスクリプト5に従って（MQ2），“VBRJP200をコピー

してよいか？”という問い合わせを端末に送り、この問い合わせが表示装置の画面に表示される。ユーザAは表示された問い合わせに対する回答を入力し、端末がその回答をホスト計算機に送り返す。ここでは、ANS=はいが送り返され、ホスト計算機はチェックスクリプト5に従って、リモートインストールを承諾し（RIS=OK）、VBRJP200.DLLのコピーを指示するフラグF2をONにする（MA2）。

【0028】もし、ファイルVBRJP200.DLLが端末の指定されたディレクトリにあった場合はANS=ONが送り返されるので、その時点でRIS=OKとなる（MA1）。

【0029】このように環境チェックを自動的に行うことにより、ユーザAの環境に適合しないソフトウェアが配送されるのを防ぐことができる。例えば、あるパッケージソフトウェアを通信回線を介して購入した後に、特定のドライバがないとそれが動作しないことを知るといったような事故が未然に防止される。

【0030】RIS=OKとなるとホスト計算機は環境チェックを終了し、判定結果（JUDGE=OK）とともに、配送先のディレクトリSOUKODIRを端末に送る。このSOUKODIRは、ユーザA環境ファイルに格納されているSOUKOのディレクトリであるD:¥SOUKOの下に、テトリスの推奨ディレクトリであるTECTをサブディレクトリとして付加した形式で指定される。

【0031】このとき同時に、インストールの可否（RIS）、インストールプログラム（インストーラ）のアイコン登録の有無（ICON）、およびダウンロードの可否（LOAD）が端末に送られる。これらのフラグRIS、ICON、LOADにより、ホスト計算機はインストール、インストーラのアイコン登録、ダウンロードのうちのどれが可能かを端末に通知する。

【0032】インストールとはユーザAの選んだソフトウェアを端末のシステム、例えばWINDOWSに登録して、端末上で使用可能にすることを意味する。したがって、この場合はそのソフトウェアの実行ファイルをWINDOWS上でアイコン登録する作業までを含む。これに対して、インストーラのアイコン登録とはインストールを実行するプログラムを端末上でアイコン登録することを意味する。

【0033】ここでは、インストールとダウンロードが許諾され（RIS=OK、LOAD=OK）、インストーラのアイコン登録は行わない（ICON=NG）という条件が提示される。複雑なインストールプログラムを持つソフトウェアの場合には、インストールが許諾される代わりにインストーラのアイコン登録が必要である旨が提示される。また、WINDOWSを搭載している端末からTOS（TOWNSのOS）用のアプリケーションを要求されたような場合には、ダウンロードのみが

許諾される。

【0034】次に、端末の端末ソフトはインストール、インストーラのアイコン登録、ダウンロードの順に優先順位をつけて、より優先順位の高いものをデフォルトとして設定し、表示装置の画面に表示する。ここでは、ホスト計算機により許諾されたインストールとダウンロードのうち優先順位のより高いインストールがデフォルトとして設定され、インストール方法選択ウィンドウに表示される。

【0035】ユーザAは表示されたインストール方法を確認して、確認した旨を入力する（ステップS15）。また、ユーザAはここで表示された設定を変更することもできる。例えば、インストーラのアイコン登録を行いたいときは、インストール方法選択ウィンドウ内の「インストーラのアイコン登録」を選択して入力する。

【0036】基本的には、ユーザAは手間をかけずにできあいのインストールを行いたい場合は「システム登録」を選択し、細かいインストール設定自分で行いたい場合は「インストーラのアイコン登録」を選択し、格納場所を後で変更したい（別の機種の端末にインストールしたい）場合は「ダウンロード」を選択する。「ダウンロード」を選択すれば、端末の機種とは異なる機種用のソフトウェアを入手して動作するかどうか試してみることも可能になる。

【0037】次に、端末はホスト計算機から指示された宅配用のサブディレクトリD：¥SOUKO¥TETを、ハードディスク内に自動的に生成する（ステップS16）。ここでもし、端末にサブディレクトリD：¥SOUKO¥TETが既に存在している場合は、例えばD：¥SOUKO¥TET 001というサブディレクトリをつくり、これも既に存在している場合はD：¥SOUKO¥TET 002というサブディレクトリをつくる。

【0038】テトリスのファイル本体6はファイルTET1.LZH(F1)とVBRJP200.DLL(F2)とから成り、TET1.LZHは4つのファイルTETRIS.EXE、TOWNS.DRV、PC98.DRV、およびMAC.DRCを圧縮（凍結）してできている。TET1.LZHを圧縮前の状態に伸長（解凍）するとこれらの4つのファイルに分かれるが、TET1.LZHの解凍はホスト計算機から端末に配送された後に行われる。

【0039】宅配用のサブディレクトリを生成した端末は、リモートインストールの開始を依頼するコマンドRIS\_INSTALLを選択したソフトウェアの番号とともにホスト計算機に送る（図46、ステップS17）。これを受けて、ホスト計算機は送られた番号に対応するソフトウェアのリモートインストールを開始する。リモートインストールは、ホスト計算機が作成したテトリスのインストールスクリプト7に従って、ホスト

計算機と端末の間のやりとりにより自動的に行われる（ステップS18）。

【0040】インストールスクリプト7には、まずファイルTET1.LZHをユーザA側の格納場所@SOUKO@へダウンロードすることを指示する記述がある。そこで、ホスト計算機は@SOUKO@をSOUKODIR=D：¥SOUKO¥TETに置き換えて、ハードディスクのサブディレクトリD：¥SOUKO¥TETにTET1.LZHをダウンロードする。

10 【0041】端末からダウンロードの完了（OK）を通知されると、次にホスト計算機は、@WINDIR@をD：¥WINDOWSに置き換えて、ハードディスクのディレクトリD：¥WINDOWSにVBRJP200.DLLをダウンロードする。

【0042】端末からダウンロードの完了（OK）を通知されると、次にホスト計算機は、格納場所@SOUKO@(D：¥SOUKO¥TET)にダウンロードしたTET1.LZHを解凍する指示、LHA X D：¥SOUKO¥TET¥TET1.LZHを送る。これを受けて、端末はTET1.LZHを前述した4つのファイルTETRIS.EXE、TOWNS.DRV、PC98.DRV、およびMAC.DRCに解凍する。これらの4つのファイルはTET1.LZHと同じサブディレクトリD：¥SOUKO¥TETに保持される。

【0043】端末から解凍の完了（OK）を通知されると、次にホスト計算機は、格納場所@SOUKO@(D：¥SOUKO¥TET)の機種@.DRVというファイルを格納場所@WINDIR@(D：¥WINDOWS)に移動させてファイル名をFONT.DRVに変更する指示、MOVE D：¥SOUKO¥TET¥TOWNS.DRV D：¥WINDOWS¥FONT.DRVを送る。

【0044】このとき、ホスト計算機はユーザA環境ファイル2を参照して、機種@をTOWNSに置き換えて送る。これを受けて、端末はサブディレクトリD：¥SOUKO¥TETのファイルTOWNS.DRVをディレクトリD：¥WINDOWSに移動し（ファイル移動）、FONT.DRVというファイル名に変更する（リネーム）。

40 【0045】端末からファイル移動およびリネームの完了（OK）を通知されると、次にホスト計算機は、ファイルTETRIS.EXEのアイコン登録を行う指示、ICON TETRIS.EXEを送る。これを受けて、端末はサブディレクトリD：¥SOUKO¥TETのファイルTETRIS.EXEをアイコン化して端末内に登録する。

【0046】これにより、表示装置の画面に表示された倉庫ウィンドウ内に、例えばTETRIS.EXEを起動するアイコンが表示され、アイコンをクリックすればテトリスが動作を開始する。

15

【0047】端末からアイコン登録の完了(OK)を通知されると、ホスト計算機はRETURNを送り返してリモートインストールの終了を端末に通知し、一連のインストール作業を終了する。リモートインストールの終了を通知された端末は、ユーザAの指示に従って次のソフトウェアの選択とそのリモートインストールを行うか、あるいは処理を終了する(ステップS19)。

【0048】このようなリモートインストールシステムを利用して、ユーザにソフトウェアを販売する場合、流通するソフトウェアを管理する従来の技術として、「ソフトウェア流通システムにおける識別子管理装置および方法」(特願平7-1798、特開平8-190529)がある。

【0049】このシステムでは、ホスト計算機はそれぞれのユーザ端末に端末識別子(マシンID: MID)を発行し、端末のユーザにはマシンIDとは別のユーザ識別子(ユーザID: UID)を発行する。また、各マシンIDに対応して端末のパスワード(マシンパスワード: MPSW)を設け、各ユーザIDに対応してユーザパスワードを設ける。

【0050】ホスト計算機はこれらのマシンID、マシンパスワード、ユーザID、およびユーザパスワードを用いて、ソフトウェアの販売先である端末とユーザの情報を管理する。

【0051】ユーザに販売したソフトウェアが何らかの原因により破壊され使用不可能となった場合には、ホスト計算機は販売記録を参照して、そのソフトウェアの復旧サービスを行う。また、販売したソフトウェアのバージョンアップのサービスも行う。さらに、ホスト計算機は端末に与えるマシンパスワードを動的に変更して、アクセスが行われるたびにそれをチェックすることにより、インストールしたソフトウェアが他の端末にコピーされたかどうかを監視する。

【0052】あるユーザから他のユーザに端末の譲渡があった場合には、その端末にインストールされたソフトウェアは、そのバージョンアップや復旧等のサービスを受ける権利も含めて譲り渡すことが可能となる。このような譲渡を行えば、不正コピーの防止にも繋がるし、権利の譲渡もスムーズに行われるため、ユーザとベンダーの双方に有益に働く。

【0053】ここで、図47から図50までを参照しながら、従来のソフトウェア流通システムにおける処理のフローを説明する。図47は、ユーザIDの登録処理のフローチャートである。処理が開始されると、まずユーザは端末を流通センターのホスト計算機に接続して(ステップS21)、名前、キャッシュカードの番号、住所等の個人情報を入力する(ステップS22)。これを受けて、ホスト計算機は仮のユーザIDと仮のユーザパスワードを発行して、ユーザの仮登録を行う(ステップS23)。ここで、ユーザは一旦ホスト計算機との接続を

16

断ち、キャッシュカードが認証されるのを待つ(ステップS4)。

【0054】キャッシュカードが認証され、流通センターから正式のユーザIDと正式のユーザパスワードとが郵送されると(ステップS25)、ユーザは再び端末をホスト計算機に接続して(ステップS26)、受け取った正式のユーザIDと正式のユーザパスワードとを入力する(ステップS27)。

【0055】これにより、ホスト計算機は正式のユーザIDとユーザパスワードを記載した郵便がユーザ本人に届いたことを確認し、そのユーザを正式に登録(本登録)して処理を終了する。このとき、郵送されたユーザパスワードと共に、別のパスワードをユーザが入力して登録することもできる。

【0056】図48は、端末IDの登録処理のフローチャートである。処理が開始されると、まずユーザは端末を流通センターのホスト計算機に接続して(ステップS31)、登録されているユーザIDとユーザパスワードを入力する(ステップS32)。その後、端末がその機種や使用OS等のマシン情報を自動的にホスト計算機に送る(ステップS33)。ホスト計算機は送られたマシン情報に端末IDと端末パスワードを付加して所定の形式で記憶し、それらの端末IDと端末パスワードを端末に送る(ステップS34)。こうして、発行された端末IDと端末パスワードは端末内にも保持される。

【0057】図49は、流通センターに登録されたユーザにネットワークを介してソフトウェアを販売する処理のフローチャートである。図49において、ユーザのリクエスト等により処理が開始されると、まずユーザの端末がネットワークに接続される(ステップS41)。次に、ホスト計算機はユーザが入力したユーザIDとユーザパスワードをチェックし(ステップS42)、それらが正しくなければ(NG)、処理を終了する。

【0058】ユーザIDとユーザパスワードが正しければ(OK)、次にホスト計算機は端末内に保持された端末IDと端末パスワードとを自動的に読み取り、これらをチェックする(ステップS43)。端末IDと端末パスワードが正しくなければ(NG)、不正コピーが行われた可能性があるので不正に対応する処理(不正処理)を行う(ステップS44)。

【0059】端末IDと端末パスワードが正しければ(OK)、商品であるソフトウェアのリストを端末の画面に表示させ、ユーザに購入する商品の選択を行わせる(ステップS45)。ユーザは表示されたリストから商品を選択し、復旧サービスの要請の場合はその旨を入力する。

【0060】次に、ホスト計算機はユーザからの要求が新規商品の購入か既に販売した商品の復旧要請かを判断し(ステップS46)、復旧要請の場合はそのユーザの購入情報を参照して、該当する商品を過去に購入してい

17

るかどうかを調べる（ステップS47）。ユーザが購入していない商品の復旧を要請している場合は（ステップS47、NO）、復旧サービスの対象とならないので再びステップS45の処理に戻る。

【0061】ユーザが過去に購入した商品の復旧を要請している場合は（ステップS47、YES）、ホスト計算機はネットワークを介してその商品を端末に宅配し、再インストールする（ステップS49）。そして、使用契約等に基づいてユーザに課金して（ステップS50）、処理を終了する。ただし、無償で復旧サービスを行なう契約が結ばれている場合は課金は行わない。

【0062】ステップS46でユーザが新規商品の購入を要求している場合は、選択された商品の販売を決定し（ステップS48）、ネットワークを介してその商品を端末に宅配してインストールする（ステップS49）。そして、商品の代金をユーザに課金して（ステップS50）、処理を終了する。

【0063】ステップS50においては、入力されたユーザIDを持つユーザに対して代金が課されるが、ユーザIDの管理はユーザに委ねられる。各ユーザはそのユーザパスワードを指定してユーザIDを管理する。

【0064】商品の販売契約がユーザを対象とせずに、インストールする端末に対して販売することになってい場合は、ステップS50において端末に対して代金が課金される。この場合は、ステップS47においてその端末が該当する商品を過去に購入しているかどうかを調べ、購入していたときにのみ復旧サービスを行う。

【0065】また、端末IDについては、ホスト計算機が端末パスワードを付加し、端末が1回接続される毎にその端末の端末パスワードを自動的に書き換えて管理する。不正コピーが行われると、書き換え前の端末パスワードと共にアクセスが行われるため、その事実を認識することが可能になる。端末IDおよび端末パスワードについては、ホスト計算機がバットレスを行うことができる。

【0066】図50は、ステップS43における端末パスワードのチェックと書き換え、およびステップS44の不正処理のフローチャートである。図50において処理が開始されると、ホスト計算機は接続された端末の端末パスワードを、その端末の前回接続時に付与した端末パスワードと比較する（ステップS51）。

【0067】それらが一致すれば、新しい端末パスワードを生成してその端末内に書き込み、ホスト計算機内にも保持しておく（ステップS52）。このとき、ホスト計算機は例えば乱数のように予想できないものを用いて、次の端末パスワードを決定する。また、書き換えられた古い端末パスワードは後で参照するために保存しておき（ステップS53）、処理を終了する。

【0068】ステップS51で2つの端末パスワードが一致しないときは、ホスト計算機は不正コピーが行われ

18

たと判断し、接続された端末に新しい端末IDを付与して新規に管理する（ステップS54）。そして、接続時における端末パスワードを保存されている古い端末パスワードと順次比較して、その端末パスワードによるアクセスがあった日時を求める（ステップS55）。これにより、不正コピーが行われたタイミングを特定して処理を終了する。

【0069】また、リモートインストールシステムにユーザが作成したソフトウェアを登録する先願の技術としては、「ソフトウェア登録システムおよび方法」（特願平7-258506）がある。

【0070】図51は、このシステム内での場の構成を示している。図51のシステムにおいては、ホスト計算機の中に仮想的につくられた、クラブと呼ばれるユーザのグループが最小単位となり、ソフトウェア情報の交換の場を形成する。クラブの構成員は会員とも呼ばれる。クラブ12、13、14は同じ階層に属し、それぞれが会議室機能とリモートインストールシステム（RIS）の機能と持っている。

【0071】これらのクラブ12、13、14の上位階層には上位クラブ11がある。この例ではクラブの階層は2階層であるが、一般的には何階層でもよい。宅配されるコンテンツとなるソフトウェアは、必ず、いずれかのクラブにアップロードされ、そこに登録される。例えば、ソフトウェア15がクラブ12にアップロードされると、クラブ12に最初に登録され、クラブ12はソフトウェア15のオリジナルクラブとなる。オリジナルクラブに登録されたソフトウェアを他のクラブに持つて行くには、転載という方法と移管という方法がある。

【0072】転載とは、ソフトウェアを他のクラブからも見えるようにすることを意味し、移管とは、オリジナルクラブの機能そのものを他のクラブに移すことを意味する。ソフトウェア15を希望する会員は、オリジナルクラブ12または転載先クラブ11、13のいずれから、それをダウンロードすることができる。

【0073】基本的には、オリジナルクラブを選ぶ権利はソフトウェア15を作成した会員が持っている。しかし、作者がソフトウェア15をアップロードして、一旦公開を許可したら、それを他のクラブに転載または移管する権利はオリジナルクラブの管理者に移る。現実の運用に当たっては、アップロードした作者や各クラブの管理者の間でこれらの権利について交渉する必要があるが、コンピュータ内の仕組みとしては、それぞれの権利をあらかじめ次のように決めておく。また、作者や各管理者の義務は、契約によって例えば次のように決められる。

(1) 一般作者の権利と義務  
コンテンツ（ソフトウェア）をアップロードする権利  
自分のアップロードしたソフトウェアを無償でテスト宅配する権利（テスト時のRISの料金が無償になる）

19.

## ソフトウェアの公開を許可する権利

自分のアップロードしたソフトウェアをサポートする義務（ソフトウェアの利用者からの質問に答えたり、エラーが発生した時の修正を行ったりする）

## (2) オリジナルクラブ管理者の権利と義務

クラブ内のソフトウェアを無償でテストする権利（テスト時のソフトウェア使用料が無償になる）

## ソフトウェアを公開する権利

## 転載先クラブに転載の許可を出す権利

## クラブ内のソフトウェアをサポートする義務

上位クラブには、特別な理由が無い限り、転載の許可を出す義務。

## (3) 転載先クラブ管理者の権利と義務

## 転載が許可されたソフトウェアを公開する権利

## クラブ内のソフトウェアをサポートする義務

## (4) 上位クラブ管理者の権利

## 転載が許可されたソフトウェアを公開する権利

上位クラブは、基本的に下位クラブのソフトウェアを転載することができるので、最上位のクラブの会員はすべてのソフトウェアを閲覧することができるようになる。また、転載先クラブの管理者がソフトウェアの使用方法等を確実にサポートしてくれる事を条件に転載するので、ソフトウェアが閲覧可能なクラブ内で、そのサポートが必ず受けられる。

【0074】ここで、図52から図54までを参照しながら、ソフトウェア登録システムにおける作者や管理者の作業の手順について説明する。図52は、作者の作業のフローチャートである。作業が開始されると、作者は、まずソフトウェアを作成し、アップロードに必要なファイル群を用意する（ステップS61）。次に、アップロードするクラブを選択し、コマンドUPLOADによりソフトウェアをアップロードして（ステップS62）、アップロード先での自動チェックの結果を受け取る（ステップS63）。

【0075】ここでは、誤動作チェック、ウィルスチェック、著作権や商標権のチェック等が自動的に行われる。チェックの結果（ステップS64）、エラーが発生すればエラー部分を修正し、修正部分のみ再びアップロードして（ステップS65）、ステップS63以降の作業を繰り返す。

【0076】そして、自動チェックが通ったら、次にRISによりテスト宅配を行う（ステップS66）。テスト宅配では、アップロードされたソフトウェアがリモートインストール時に問題を起こさないかどうかがチェックされる（ステップS67）。テスト宅配でエラーが発生すればエラー部分を修正し、その部分のみ再びアップロードして（ステップS68）、ステップS66以降の作業を繰り返す。テスト宅配で合格したら、PUSHによりソフトウェアの公開を許可し（ステップS69）、作業を終了する。

20.

【0077】図53は、オリジナルクラブの管理者の作業のフローチャートである。作業が開始されると、管理者は、まず作者により公開を許可されているソフトウェアをテスト宅配し（ステップS71）、問題が無いかチェックする（ステップS72）。テスト宅配で問題がなければ、コマンドPUBLISHによりソフトウェアをオリジナルクラブの会員に公開し（ステップS73）、問題があればそれを作者に連絡して（ステップS74）、作業を終了する。

10 【0078】図54は、転載先クラブの管理者の作業のフローチャートである。作業が開始されると、管理者は、希望するソフトウェアがあったら、その転載許可をオリジナルクラブに依頼する（ステップS81）。依頼に対する応答を受け取り（ステップS82）、転載が許可されなければそのまま作業を終了する。コマンドPREMITにより転載が許可されれば、コマンドLINKによりそのソフトウェアを自分のクラブに転載する（ステップS83）。この時、自分のクラブで検索しやすいようにキーワードを変更しておく。

20 【0079】次に、転載したソフトウェアをテスト宅配し（ステップS84）、問題が無いかチェックする（ステップS85）。テスト宅配で問題がなければ、コマンドPUBLISHによりソフトウェアをクラブの会員に公開し（ステップS86）、問題があればそれをオリジナルクラブに連絡して（ステップS87）、作業を終了する。

【0080】ところで、パソコン通信で流通しているソフトウェアには、様々な種類のものがある。例えば、フリーウェアと呼ばれるものは基本的に無料で配布され、シェアウェアと呼ばれるものは機能制限付きで一旦無料で送付された後、所定の代金が送金されれば機能制限が解除されることになっている。また、商品として販売されているものは、基本的に代金と引き換えに送付される。

30 【0081】配送センターがリモートインストールの機能を利用して、ソフトウェアをユーザに販売するサービスを行う場合、このような多様な販売形態に対応して、代金を確実に受け取ることを保証する機構が必要になる。このような代金の決裁に関する先願としては、「ソフトウェア代金決裁システムおよび方法」（特願平7-258507）がある。

【0082】図55は、このシステムで用いられるファイル群のアップロード処理の例を示している。シェアウェアの作者は、まず本体登録ファイルとして、CFGファイル21(AAA.CFG)、説明ファイル22(AAA.TXT)、インストール関連ファイル23(ここではアイコンファイルICON.DEF)、および本体ファイル24(AAA.LZH)を自分の端末からアップロードする。

50 【0083】ホスト計算機は、これらのアップロード情

21

報をコンテンツデータベース28に登録する。ここでは、アップロードされたソフトウェア「AAAスケジューラ」のソフトコード、名称、タイプ(TYPE)、本体ファイル名、説明ファイル名、アイコンファイル名等が管理情報として登録されている。タイプの欄のS H A R Eはソフトウェアの種類がシェアウェアであることを表す。コンテンツデータベース28は、例えば、ホスト計算機内または外部のディスク装置内に設けられる。

【0084】次に、作者は送金手続きファイルとして、定義ファイル25(AAAS.CFG)、CHKファイル26(AAAS.CHK)、および書換えファイル27(INI.DEF)をアップロードする。これにより、送金手続きファイルAAASのソフトコード、名称、タイプ、CHKファイル名、後処理用のファイル名等がコンテンツデータベース28に登録される。

【0085】後処理用のファイルとして、ここでは、書換えファイル27のファイル名INI.DEFが記されている。また、タイプの欄のSOKIN#RISは、ソフトウェアの種類がシェアウェアの送金手続きファイルであることを表し、AAAS.CFGの[instepte]セクションに記述された情報に対応している。

【0086】次に、図56、57、58、59を参照しながら、アップロードされたファイル群を用いたシェアウェアの送金手続きについて説明する。シェアウェア手続きにおいては、上述のリモートインストールの手続きに加えて、プロトコル上に送金フラグを設ける。そして、端末からこのフラグを立ててソフトウェアの検索を要求することにより、シェアウェア手続きを選択できるようになる。また、端末の画面に送金フラグをON/OFFするメニューを表示させる。

【0087】この例において、シェアウェア「AAAスケジューラ」は、送金手続きの前に、機能制限付きでユーザシステムにインストールされているものとする。ユーザがこのソフトウェアを購入しようとした時は、ホスト計算機と端末の間で次のようなコマンド/レスポンスのやりとりを行う。

【0088】端末は、まずユーザ環境をホスト計算機に送信し(図56、ステップS91)、ホスト計算機はこれを受信すると応答を返す(ステップS92)。次に、ユーザがソフトウェア検索用のキーワードリストを要求すると(ステップS93)、ホスト計算機はキーワードリストを返送する(ステップS94)。

【0089】このとき、図57に示すように、端末の画面上にはオプション手続きのメニュー29が表示され、ユーザはその中から「送金」を指定し、キーワードリストの中からキーワードを選択する。これにより、送金フラグSOKINが立てられ(オンになり)、シェアウェアの検索を開始する指示がホスト計算機に送られる(図57、ステップS95)。

【0090】ホスト計算機は、指定されたキーワードで

22

コンテンツデータベース28を検索し、タイプがSOKINで始まるソフトウェアの名称とその送金手続きファイル(送金ソフト)のソフトコードとを返す(ステップS96)。ここでは、「AAAスケジューラ」、「BBBスケジューラ」等の名称および送金ソフトのソフトコード4000、4001等が返送されている。

【0091】端末は送金ソフトのみリストアイングし、ユーザはリストアイングされた中の特定の送金ソフトを指定する(ステップS97)。ここでは、ソフトコード4000が指定されている。ホスト計算機は、ソフトコード4000の送金ソフトの条件により端末側とネゴシエーションを行う(ステップS98)。ここでは、まず、コマンドST4を用いて、ユーザシステム内に格納された初期設定ファイルAAA.INIの位置を調べるように端末に指示する。

【0092】これを受けて、端末はAAA.INIの場所を調べ、その場所はE:¥AAAということをホスト計算機に通知する(ステップS99)。ST4というコマンドは、あらかじめ端末側に具備されているものとする。

【0093】次に、ホスト計算機はダイアログBOX30を端末の画面に表示させ、AAA.INIの位置はE:¥AAAでよいかどうかをユーザに確認する(図58、ステップS100)。ダイアログBOX30に表示されたディレクトリが正しければ、ユーザはそのディレクトリをそのまま返送し(ステップS101)、ホスト計算機は、ユーザシステムの書き換えるべきファイルのディレクトリパスはE:¥AAA¥AAA.INIと確定する。

【0094】もし、表示されたディレクトリが正しくなければ、ユーザは正しいディレクトリ名を入力する。例えばG:¥GGGと入力すると、端末はディレクトリパスG:¥GGG¥AAA.INIをホスト計算機に返す。AAA.INIの格納場所が確定したので、ホスト計算機は、シェアウェア送金が可能であることを端末に通知する(ステップS102)。

【0095】次に、ユーザは機能制限の解除を要求する(図59、ステップS103)。これを受けて、ホスト計算機は、定義ファイル25の[instepte]セクションを参照し、代金をそのユーザの口座等から引き落とした後に、AAA.INIの書換え手順が記述されている書換えファイルINI.DEFを送付する。さらに、定義ファイルの[last]セクションを参照して後処理のコマンドCHGINIを送り、INI.DEFの手順に従って書換えを行なうことを端末に指示する。

【0096】これを受けて、端末はダウンロードされたINI.DEFを参照し、AAA.INIを書換える。これにより、シェアウェア「AAAスケジューラ」の機能制限が解除され、ユーザシステム上で完全に動作するようになる。その後、ホスト計算機はINI.DEFを

端末から削除して、処理を終了する。

【0097】この例では、定義ファイル25の[*ins type*]のセクションにその場で制限解除を行うという情報が記されていたので、代金の引き落としと同時にシェアウェアの機能制限を解除した。しかし、一般的なパソコン通信センターと同様に、ホスト計算機が代金引き落としとシェアウェア登録者への電子メールの発行だけを行う構成とすることもできる。

【0098】図60、61、62は、このようなソフトウェア「BBBスケジューラ」の代金引き落とし手続きを示している。ただし、この手続きの前に、シェアウェア「BBBスケジューラ」は機能制限付きでユーザシステムにインストールされているものとする。ユーザがこのソフトウェアを購入しようとした時は、ホスト計算機と端末の間で次のようなコマンド/レスポンスのやりとりを行う。

【0099】端末は、まずユーザ環境をホスト計算機に送信し(図60、ステップS111)、ホスト計算機はこれを受信すると応答を返す(ステップS112)。次に、ユーザがソフトウェア検索用のキーワードリストを要求すると(ステップS113)、ホスト計算機はキーワードリストを返送する(ステップS114)。

【0100】このとき、図61に示すように、端末の画面上にはオプション手続きのメニュー29が表示され、ユーザはその中から「送金」を指定し、キーワードリストの中からキーワードを選択する。これにより、送金フラグSOKINが立てられ、シェアウェアの検索を開始する指示がホスト計算機に送られる(図61、ステップS115)。

【0101】ホスト計算機は、指定されたキーワードでコンテンツデータベース28を検索し、タイプがSOKINで始まるソフトウェアの名称とその送金ソフトのソフトコードとを返す(ステップS116)。端末は送金ソフトのみリストイングし、ユーザはリストイングされた中からソフトコード4001の送金ソフトを指定する(ステップS117)。

【0102】次に、ホスト計算機はメッセージ31を端末の画面に表示させ、課金してよいかどうかをユーザに確認する(図62、ステップS118)。このとき、ホスト計算機は、定義ファイルの[*inst type*]セクションを参照し、フラグSOKINの値をメール発行のみを表す「0x08」に変更して、端末に返送する。

【0103】ユーザは、課金されてもよければOKを、購入しない場合はNGを選択する。ここでは、OKが選択され、登録者に対するメールの発行の依頼が端末からホスト計算機に送られる(ステップS119)。

【0104】これを受け、ホスト計算機は代金をそのユーザの口座等から引き落とし、「BBBスケジューラ」の登録者に代金引き落としを知らせる電子メールを送る。メールの送付先としては、定義ファイルの[*ty*

[*pe*]セクションに記述された送金先FJOKIを用いる。

【0105】ホスト計算機から電子メールを受け取った登録者は、電子メール等の手段により、ソフトウェアの購入者に機能制限解除の方法を連絡する。これにより、購入者は「BBBスケジューラ」のすべての機能を使用することができるようになる。

【0106】

【発明が解決しようとする課題】しかしながら、上述の10ような従来のリモートインストールシステムには、次のような問題がある。

【0107】販売されるソフトウェアは秘密の情報であるため、セキュリティの確保された回線を介して宅配する必要がある。したがって、あらかじめセキュリティの確保が保証されないインターネット上に適用するためにハッキング防止のための対策を施す必要がある。

【0108】また、インターネット上の情報探索用ソフトウェアツールであるWWWブラウザ(world wide web browser)と、リモートインストールシステムとの連携方法としては、様々な機構が考えられ、提供するサービスに応じて適した機構を構築する必要がある。

【0109】また、従来のリモートインストールシステムにおける端末のマシンIDは、ホスト計算機がただ一つしか存在しないことを前提として作成/管理されている。このため、複数のホスト計算機をRISサーバとしてサービスを行うと、同じマシンIDを各ホスト計算機がそれぞれ異なる端末に付与する可能性がある。この場合、ホスト計算機が端末を誤って識別するという問題が生じる。

【0110】さらに、インターネット上では識別情報等も盗用される恐れがあるため、通信相手を正確に識別することが困難である。このため、第3者が不正に入手した識別情報をを利用して、RISのホスト計算機になりますことができる。このような場合、ユーザがそれを見破ることができる必要がある。

【0111】本発明の課題は、インターネット上でリモートインストールシステムを利用して、安全かつ適切な会員制サービスを実現するシステムおよびその方法を提供することである。

【0112】

【課題を解決するための手段】図1は、本発明のサービスシステムの原理図である。図1のサービスシステムは、本発明の第1、第2、第3、第4、第5、第6、第7、第8、第9、第10、および第11の原理を含む。

【0113】第1の原理において、サービスシステムは、登録手段80、キー情報付与手段81、および暗号化手段82を備え、ソフトウェア配達サービスを提供する。登録手段80は、セキュリティの確保された通信路を介して、クライアントのサインアップを行い、キー情報付与手段81は、上記サインアップの過程で、上記ク

25

ライアントのマシン識別子に対応したキー情報を付与する。そして、暗号化手段82は、上記キー情報を用いて、インターネット上のパスワードとソフトウェアコンテンツのうち少なくとも一方の暗号化を行う。

【0114】暗号化に用いられるキー情報は、セキュリティの確保された通信路を介してやり取りされるので、盗用されることがない。こうして付与された秘密のキー情報を用いてパスワードを暗号化することで、インターネット上において、リモートインストールシステムへのログインシーケンスのセキュリティを高めることができる。また、このキー情報を用いてコンテンツを暗号化することで、インターネット上において、リモートインストールのシーケンスのセキュリティを高めることができる。

【0115】第2の原理において、サービスシステムは、リモートインストール手段83とブラウザ手段88を備え、ソフトウェア配達サービスを提供する。リモートインストール手段83は、ホームページ上のアンカーファイルにより指定されるソフトウェアを、自動的にサーバからクライアントに配達し、ブラウザ手段88は、上記アンカーファイルがアクセスされたとき、自動的にリモートインストール手段83を起動する。

【0116】ブラウザ手段88がリモートインストール手段83を起動することで、ユーザが指定したソフトウェアが自動的に配達される。したがって、ユーザはリモートインストール手段83を意識することなく、インターネットのホームページ上でリモートインストールサービスを利用することができる。

【0117】第3の原理において、サービスシステムは、課金手段84とブラウザ手段88を備え、オンラインショッピングサービスを提供する。課金手段84は、自動的にクライアントからサーバへ接続して、ホームページ上のアンカーファイルにより指定される商品またはサービスの課金処理を行い、ブラウザ手段88は、上記アンカーファイルがアクセスされたとき、自動的に課金手段84を起動する。

【0118】課金手段84としては、例えばリモートインストールシステムが用いられ、ブラウザ手段88が課金手段84を起動することで、ユーザが指定した商品またはサービスの課金が自動的に行われる。したがって、インターネット上でリモートインストールシステムを利用したオンラインショッピングサービスが実現される。

【0119】第4の原理において、サービスシステムは、処理手段85とブラウザ手段88を備え、通信サービスを提供する。処理手段85は、ホームページ上のアンカーファイルにより指定される通信サービスの課金処理を行い、その通信サービスを利用するため必要な情報を、自動的にサーバからクライアントへ送る。また、ブラウザ手段88は、上記アンカーファイルがアクセスされたとき、自動的に処理手段85を起動する。

26

【0120】処理手段85としては、例えばリモートインストールシステムが用いられ、ブラウザ手段88が処理手段85を起動することで、ユーザが指定した通信サービスの課金と、そのサービスを利用するため必要な情報の提供が自動的に行われる。したがって、インターネット上でリモートインストールシステムを利用した通信サービスが実現される。

【0121】第5の原理において、サービスシステムは、ヘルパ手段86、処理手段87、およびブラウザ手段88を備え、トランザクションサービスを提供する。ブラウザ手段88は、インターネットにアクセスし、ヘルパ手段86は、ブラウザ手段88により起動され、トランザクションサービスの一部の処理を行う。また、処理手段87は、ブラウザ手段88により起動され、ヘルパ手段86と連携して、トランザクションの使用権の付与および課金に関する処理を行う。

【0122】処理手段87としては、例えばリモートインストールシステムが用いられ、ブラウザ手段88がヘルパ手段86と処理手段87を起動し、ヘルパ手段86と処理手段87が連携することで、ユーザに対するトランザクション処理の使用権の付与と課金とが自動的に行われる。したがって、インターネット上でリモートインストールシステムを利用したトランザクションサービスが実現される。

【0123】第6の原理において、サービスシステムは、処理手段89とトランザクション手段91を備え、トランザクションサービスを提供する。トランザクション手段91は、トランザクションサービスの処理を行い、処理手段89は、トランザクション手段91により起動され、トランザクション手段91と連携して、トランザクションの使用権の付与および課金に関する処理を行う。

【0124】処理手段89としては、例えばリモートインストールシステムが用いられ、トランザクション手段91が処理手段89を起動し、それと連携することで、ユーザに対するトランザクション処理の使用権の付与と課金とが自動的に行われる。したがって、ブラウザを介すことなく、リモートインストールシステムを利用したトランザクションサービスが実現される。

【0125】第7の原理において、サービスシステムは、処理手段90とトランザクション手段91を備え、トランザクションサービスを提供する。トランザクション手段91は、トランザクションサービスの処理を行い、処理手段90は、トランザクション手段91により起動され、自動的にクライアントからサーバへ接続して、上記トランザクションサービスに必要なデータを取得する。

【0126】処理手段90としては、例えばリモートインストールシステムが用いられ、トランザクション手段91が処理手段90を起動する。処理手段90はサーバ

からデータを取得してトランザクション手段91に渡し、トランザクション手段91は、そのデータを用いてトランザクションサービスの処理を行う。したがって、ブラウザを介することなく、リモートインストールシステムを利用したトランザクションサービスが実現される。

【0127】第8の原理において、サービスシステムは、受信手段92と判定手段93を備える。受信手段92は、クライアントから、サーバ識別子とクライアント識別子を合成して生成されたマシン識別子を受け取る。そして、判定手段93は、上記マシン識別子をサーバ部とクライアント部に分解し、そのサーバ部に記述されたサーバ識別子をチェックして、上記クライアントとの接続が正しいかどうかを判定する。

【0128】クライアントがマシン識別子にサーバ識別子を混ぜて送ることで、判定手段93は、その接続要求がどのサーバに対するものかを特定することができる。そして、サーバ識別子に対応するサーバが、クライアントの正しい接続先と判定される。したがって、複数のサーバがサービスを提供する環境において、同じクライアント識別子が2つ以上のクライアントに付与された場合でも、サーバがクライアントを確実に識別することが可能になる。

【0129】第9の原理において、サービスシステムは、生成手段94、格納手段95、および接続手段96を備える。生成手段94は、サーバ識別子とクライアント識別子を合成して、クライアントのマシン識別子を生成し、格納手段95は、そのマシン識別子を格納する。そして、接続手段96は、そのマシン識別子を用いてサーバに接続する。

【0130】生成手段94がサーバ識別子を含むマシン識別子を生成し、接続手段96がそのマシン識別子を用いてサーバに接続することで、サーバは、その接続要求がどのサーバに対するものかを特定することができる。したがって、第8の原理と同様に、サーバがクライアントを確実に識別することができる。

【0131】第10の原理において、サービスシステムは、通信手段97と認証手段98を備える。通信手段97は、サーバへのログイン時に、そのサーバの認証鍵に基づく電子署名機能を用いて暗号化された指定情報を送受信し、認証手段98は、その指定情報を介してサーバの認証を行う。

【0132】サーバは、例えばリモートインストールサービスを提供し、ログインシーケンスにおいて、クライアントから指定された情報を秘密鍵で暗号化して送り返す。認証手段98は、その指定情報を対応する公開鍵で復号化し、その結果に基づいてサーバが正しいかどうかを判断する。復号化された情報が元の指定情報と一致すれば、サーバは正しいと判定される。

【0133】正しいサーバのみが正しい暗号化を行うこ

とができるので、インターネット上において、クライアントがサーバを確実に識別することが可能になる。また、クライアントが公開鍵で暗号化した指定情報をサーバに送り、サーバがそれを秘密鍵で復号化して送り返しても、同様の効果が得られる。

【0134】第11の原理において、サービスシステムは、格納手段99と接続手段100を備え、リモートインストールサービスを提供する。格納手段99は、クライアント側に設けられ、インターネット上におけるサーバのアドレス情報を格納し、接続手段100は、上記アドレス情報を用いて、自動的に上記クライアントから上記サーバに接続する。

【0135】リモートインストールシステムのサーバのアドレス情報（ドメイン名やポート番号）が、ホームページ上ではなく、ユーザ端末内の格納手段99に格納されているので、他のユーザに知られることがない。このアドレス情報を、RIS会員になったユーザの端末にのみ格納することで、インターネット上において、会員制のリモートインストールサービスが実現される。

【0136】このように、図1のサービスシステムによれば、インターネット上でリモートインストールシステムを利用した様々な会員制サービスを、安全かつ適切に提供することが可能になる。

【0137】図1の登録手段80、キー情報付与手段81、暗号化手段82、リモートインストール手段83、ブラウザ手段88、課金手段84、処理手段85、ヘルパ手段86、処理手段87、処理手段89、処理手段90、トランザクション手段91、受信手段92、判定手段93、生成手段94、接続手段96、格納手段95、通信手段97、認証手段98、格納手段99、および接続手段100は、例えば、後述する図2におけるホスト計算機111およびユーザ端末113の持つ機能に対応する。

【0138】

【発明の実施の形態】以下、図面を参照しながら、本発明の実施の形態を詳細に説明する。図2は、実施形態のサービスシステムの構成図である。図2のサービスシステムは、インターネット117に接続されたホスト計算機111およびユーザ端末113を備える。ホスト計算機111とユーザ端末113は、インターネット117以外にも、セキュリティの確保された通信路（パイプ）であるFENICS回線116を介して互いに接続されている。

【0139】ホスト計算機111は、リモートインストールサービスを提供するソフトウェアとして、RISサーバ112を搭載し、ユーザ端末113は、WWWブラウザ114の他に、リモートインストールサービスを利用するソフトウェアとして、RISクライアント115を搭載する。

【0140】図3は、図2のホスト計算機111および

29

ユーザ端末113に対応する情報処理装置(コンピュータ)の構成図である。図3の情報処理装置は、CPU(中央処理装置)121、メモリ122、入力装置123、出力装置124、外部記憶装置125、媒体駆動装置126、ネットワーク接続装置127を備え、これらの各装置はバス128により互いに結合されている。

【0141】CPU121は、メモリ122を利用してプログラムを実行し、サービスに必要な処理を実現する。メモリ122には、サービスに必要なプログラムとデータが格納され、メモリ112としては、例えばROM(read only memory)、RAM(random access memory)等が用いられる。

【0142】入力装置122は、例えばキーボード、ポインティングデバイス等に相当し、ユーザからの要求や指示の入力に用いられる。また、出力装置124は、表示装置やプリンタ等に相当し、サービス画面等の出力に用いられる。

【0143】外部記憶装置125は、例えば、磁気ディスク装置、光ディスク装置、光磁気ディスク装置等である。この外部記憶装置125に、上述のプログラムとデータを格納しておき、必要に応じて、メモリ122にロードして使用することもできる。また、外部記憶装置125はデータベースとしても使用される。

【0144】媒体駆動装置126は、可搬記録媒体129を駆動し、その記憶内容にアクセスする。可搬記録媒体129としては、メモリカード、フロッピーディスク、CD-ROM(compact disk read only memory)、光ディスク、光磁気ディスク等、任意のコンピュータ読み取り可能な記録媒体を使用することができる。この可搬記録媒体129に、上述のプログラムとデータを格納しておき、必要に応じて、メモリ122にロードして使用することもできる。

【0145】ネットワーク接続装置127は、FENICS回線116やインターネット117への接続に用いられ、通信に伴うデータ変換等を行って、他の情報処理装置(ホスト計算機111またはユーザ端末113)との間でプログラムやデータの送受信を行う。また、情報処理装置は、外部の情報提供者のデータベース130等からネットワークを介して、上述のプログラムとデータを受け取り、必要に応じて、メモリ122にロードして使用することもできる。

【0146】本実施形態では、システムへの登録手続き(サインアップ)は、必ずセキュリティの確保されたバイブで行う。そして、サインアップの過程で、RISサーバ112は、ユーザID/パスワードおよびマシンID/パスワードとともに、マシンIDに対応したインターネット用の暗号キーをRISクライアント115に付与する。この暗号キーを用いて、インターネット上のパスワードおよびコンテンツの暗号化/復号化が行われる。

30

【0147】このようなサービスを実現するため、図47、48のサインアップのシーケンスに図4に示すようなシーケンスを追加し、RISサーバ112が、端末(マシン)113にユニークに対応した秘密キー(例えばDESキー)を、端末113に付与する。

【0148】図4において、RISクライアント115が、マシンID(MID)なしでコマンドRES\_SENDENVをRISサーバ112に送ると、RISサーバ112は、秘密キーデータベース131を参照してレスポンスを返す。秘密キーデータベース131には、あらかじめMIDと秘密キーの対応表が格納されている。

【0149】ここでは、レスポンスとして、MID=1234、MP SWD=ASDF、KEY=9876がRISクライアント115に返される。このうち、KEYが秘密キーに対応する。RISクライアント115は、受け取ったこれらの情報を初期設定ファイル132(RIS.INI)に書き込んで保存する。

【0150】さらに、この初期設定ファイル132には、図5に示すように、インターネット117を介してRISサーバ112に接続するためのアドレス(ドメイン名)およびTCP/IP(transmission control protocol/internet protocol)のポート番号が記述されている。

【0151】これらのアドレスとポート番号は、ユーザがRIS会員になって、RISクライアント115が端末113にインストールされた時に、端末113の初期設定ファイル132に書き込まれる。アドレス情報が、インターネット上ではなく、RISクライアント115側に保持されているので、会員以外の他のユーザにハッキングされることはない。したがって、RIS会員のみがRISサーバ112にアクセスすることができる。

【0152】このアドレス情報を用いたインターネット117でのログインは、図6に示すようなシーケンスにて行われる。RISサーバ112からユーザID(UID)の入力指示を受け取ると、RISクライアント115は、まず、UIDとともにMIDを送出する。

【0153】RISサーバ112は、Challenge発生関数133を用いて、毎回異なる乱数Challengeを生成し、RISクライアント115に送る。

40 この乱数はRISサーバ112の識別情報として送られるが、毎回異なるため、他人がハッキングして使用することができない。したがって、他のサーバがRISサーバ112になりますことを防止できる。

【0154】RISクライアント115は、合成関数134を用いて、RISサーバ112から送られたChallengeとサインアップ時に取得したKEYとを合成し、暗号化キーを生成する。合成関数134としては、例えばEOR(exclusiveor)が用いられる。そして、その暗号化キーをDES(Data Encryption Standard)アルゴリズムの秘密キー(DESキー)として用い

31

て、ユーザパスワードを暗号化プログラム135により暗号化し、RISサーバ112に送出する。

【0155】RISサーバ112は、RISクライアント115に送ったChallengeおよびKEYから同様にしてDESキーを合成する。そして、復号化プログラム136により、暗号化されたユーザパスワードを復号化し、ユーザパスワードの確認を行う。ユーザパスワードが暗号化されてやり取りされるため、インターネット117上でのログイン時において、ユーザパスワードの盗用が防止される。

【0156】また、インターネット117上のコンテンツの配送においては、図44、45、46の従来のリモートインストール方法を図7に示すように拡張する。まず、RISクライアント115が、インターネット117を介して、セキュリティを要求されるコンテンツのデストリビューションを要求すると、RISサーバ112は、代金の与信を行う。

【0157】次に、RISサーバ112は、圧縮されたコンテンツファイルABC.LZHを、MIDに対応する秘密キーを用いて暗号化プログラム135により暗号化し、RISクライアント115にダウンロードする。そして、暗号化されたコンテンツファイルABC.DESを復号化するコマンドを送る。

【0158】RISクライアント115は、コンテンツファイルABC.DESを、保持しているKEYを用いて復号化プログラム136により復号化し、ファイルABC.LZHを取り出す。次に、RISサーバ112からのコマンドに従って、ファイルABC.LZHを解凍し、実行用ファイルABC.EXEを生成する。その後、ABC.DESとABC.LZHは自動的に消去される。

【0159】このように、あらかじめセキュリティの確保された通信路を介して秘密キーを送ることで、DESアルゴリズムのように堅牢な暗号化アルゴリズムを採用することが可能になる。また、暗号化アルゴリズムとしては、秘密キーを用いる他の任意のアルゴリズムを用いることができる。

【0160】次に、ブラウザのヘルパ・アプリケーションを起動することにより、指定されたソフトウェアを配信するリモートインストールシステムについて述べる。このシステムでは、RISクライアント115をWWWブラウザ114にヘルパ・アプリケーションとしてあらかじめ登録しておく。ここで、ヘルパ・アプリケーションとは、WWWブラウザ114からキックされて起動し、それに組み込まれた機能以外の形式のファイルを表示することのできるプログラムを意味する。

【0161】そして、ホームページ上にヘルパ起動のためのアンカーファイルを置き、そのアンカーファイルをユーザがポインティング・デバイスでクリックすると、RISクライアント115が自動的にRISサーバ11

2に接続し、指定のソフトウェアが配信されるようにする。

【0162】図8は、このようなインターネット117上のソフトウェア配信システムを示している。ソフトウェアのベンダであるソフト工房141は、インターネット117上にホームページ142を開き、自社の開発したソフトウェアの宣伝を行う(処理P1)。それとともに、自社の開発したソフトウェアを、図51、52に示した先願の方法でRISサーバ112に登録する(処理P1)。

【0163】このホームページ142を構成するHTML(hypertext markup language)ファイルは、図9のように記述される。これにより、“競馬ソフト”、“ペチンコソフト”等のソフトウェア名とそれらの配信を受けるための選択ボタン(Risアイコン)が表示される。これらのRisボタンには、それぞれヘルパ起動のためのアンカーファイルがリファレンスとして設定されている。

【0164】例えば、“競馬ソフト”的Risアイコン20には、図10に示すようなアンカーファイル144(KEIBA.RIS)がリンクされている。このKEIBA.RISの[RIS]セクションには、ソフトウェア名とソフトウェア番号(Soft)とが記述される。

【0165】また、アンカーファイル144におけるWWWサーバのMIME(multipurpose internet mail extensions)設定として、ファイルタイプ“.RIS”がMIMEタイプ“application/x-ris”に対応付けられる。MIMEとは、WWWにおいて様々なファイル形式を扱うための方法である。これにより、WWWブラウザ114がこのリファレンスを参照してきたとき、対応するWWWサーバが、MIMEタイプとして“application/x-ris”を返すようになる。

【0166】ユーザ側は、図47、48、4の方法にて、RIS会員として既にユーザID/パスワードおよびマシンID/パスワードが付与されているものとする。また、WWWブラウザ114に、RISクライアント115をヘルパ・アプリケーションとして登録しておこう。

【0167】例えば、WWWブラウザ114としてNetscapeを用いた場合は、File-Typeとして“.RIS”を登録し、MIME-TYPEとして“application/x-ris”を登録する。また、RISクライアント115を起動するLaunchアプリケーションとして、“C:\RISW410\RISWIN32\RISANC32.EXE”と登録する。

【0168】この状態で、ユーザがソフト工房ホームページ142にアクセスし(処理P2)、“競馬ソフト”

50

33

の横のR i sアイコン143を、ポインティング・デバイスでクリックしたとする（処理P3）。このとき、WWWブラウザ114は、自動的にR I Sクライアント115を起動し、R I Sクライアント115にファイルKEIBA.R I Sの内容を渡す（処理P4）。

【0169】起動されたR I Sクライアント115は、図6に示した方法でR I Sサーバ112に接続する（処理P5）。そして、ログイン後は、図11に示すように、図44、45、46と同様のシーケンスで、R I Sサーバ112がソフトウェアのデストリビューションを行う。このとき、ファイルKEIBA.R I Sから抽出されたソフトウェア番号が、R I Sクライアント115からR I Sサーバ112に送られ、それに対応するソフトウェアが自動的に端末113に配達される。

【0170】以上の操作が行われると、R I Sサーバ112上のデータベースには、図12の購入テーブルおよび図13の支払いテーブルに記述されたような購入履歴が残る。そこで、R I Sサーバ112は、この購入テーブルを元に、クレジット会社経由で購入者から代金を徴収し、支払いテーブルを元に、ベンダに払いもどしを行う（処理P6）。

【0171】このように、R I Sクライアント115をWWWブラウザ114から起動されるヘルパ・アプリケーションとして登録しておくことで、インターネット117上でのソフトウェア配達システムが実現される。また、R I Sクライアント115をヘルパとして組み込む代わりに、それをWWWブラウザ114のプラグイン（ブラウザウィンドウ内のアプリケーション）として登録しておいてもよい。

【0172】次に、ブラウザのヘルパ・アプリケーションを起動することにより、物品の購入を簡便に行うことのできるオンラインショッピングシステムについて述べる。このシステムでは、R I Sクライアント115をWWWブラウザ114にヘルパとして登録するとともに、ホームページ上にヘルパ起動のためのアンカーファイルを置く。

【0173】そして、このアンカーファイルをユーザがクリックすると、自動的にR I Sクライアント115がR I Sサーバ112に接続し、R I Sサーバ112は自動的に指定の商品の課金処理を行って、ベンダに購入報告を行う。ベンダは、これを受けて商品をユーザに発送する。

【0174】図14は、このようなオンラインショッピングシステムを示している。ベンダであるα商店151は、インターネット117上にホームページ152を開き、自社の扱う“タオルセット”や“ハンカチーフ”等の商品の宣伝を行う（処理P11）。それとともに、商品の購入処理のソフトウェアを、図51、52に示した先頭の方法でR I Sサーバ112に登録する（処理P12）。

34

【0175】ホームページ152のHTMLファイルは、図9と同様の形式で記述され、商品の選択／購入に必要なR i sアイコンをホームページ152上に表示させる（処理P13）。それぞれのR i sアイコンにリンクしたアンカーファイルおよびユーザ側のMIME等の設定は、上述のソフトウェア配達システムと同様である。例えば、R i sアイコン153には、アンカーファイル154（TOWEL.R I S）がリンクされている。

10 【0176】この状態で、ユーザがα商店ホームページ152にアクセスし（処理P14），“タオルセット”的横のR i sアイコン153をクリックしたとする（処理P15）。このとき、WWWブラウザ114は、ヘルパとして登録されたR I Sクライアント115を起動し、R I Sクライアント115にファイルTOWEL.R I Sの内容を渡す（処理P16）。

【0177】起動されたR I Sクライアント115は、R I Sサーバ112に接続し、暗号化されたパスワードでログインして、登録されたリモートインストール処理20（R I S\_INSTALLED）を開始する（処理P17）。ログイン時の設定内容や手順も、上述のソフトウェア配達システムと同様である。

【0178】開始されたリモートインストール処理では、ソフトウェアの宅配の場合とは異なる動作を行うよう、そのスクリプトを記述しておく。この場合、具体的には、ユーザへ受付票を送付する処理とベンダへ購入通知を送付する処理とが、ソフトウェア配達処理の代わりに記述される。また、必要であれば、商品の発送先をユーザが指定できるようにしておく。

30 【0179】受付票は、ソフトウェアをダウンロードする場合と同様の方法でユーザへ送付される（処理P18）。また、購入通知は、電子メールや専用回線を介した規定フォーマットの通知票としてベンダへ送付される（処理P18）。購入通知の送付処理は、ベンダ側から見ると商品の受注処理となる。この購入通知送付処理も、リモートインストール処理中に即時に実行される。

【0180】図15は、これらの送付処理のシーケンスを示している。まず、R I Sクライアント115は、ファイルTOWEL.R I Sから抽出したソフトウェア番号を、注文する商品の番号としてR I Sサーバ112に送る。このとき、コマンドR I S\_CHKENVを利用する。

40 【0181】次に、R I Sサーバ112が、レスポンスとして商品の発送先を問い合わせてくると、ユーザは希望する住所／宛て名を入力する。入力された発送先は、コマンドR I S\_CHKENVを利用してR I Sサーバ112に送られる。そして、R I Sサーバ112から“OK”が返されると、R I Sクライアント115がコマンドR I S\_INSTALLEDを送る。

50 【0182】このとき、R I Sサーバ112は、受付票

35

をダウンロードし、購入通知をベンダに送付する。そして、購入通知を受け取ったベンダは、所定の方法でユーザーに商品を発送する（処理P19）。図15の処理が終了すると、図12、13と同様の購入テーブル、支払テーブルが作成されるので、RISサーバ112は、これらを元にユーザーから代金を徴収し、ベンダへの支払いを行なう（処理P20）。

【0183】このように、RISクライアント115をWWWブラウザ114から起動されるヘルパ・アプリケーションとして登録しておくことで、インターネット117上でのオンラインショッピングシステムが実現される。また、RISクライアント115をWWWブラウザ114のプラグインとして登録しておくことも可能である。

【0184】このようなシステムによれば、RIS会員としてのユーザー情報があらかじめ登録されているので、ユーザーは商品の購入に際し、気に入った商品のボタンを押すだけでよい。このため、非常に簡便なオンラインショッピングが可能となる。また、登録時の連絡先と異なる発送先を指定することもでき、例えば、商品を第3者への贈答品として配送させることもできる。

【0185】また、RISのセンターは、販売に関わる一部の業務をアウトソーシングの形で請け負うことが可能である。したがって、RIS会員のみに商品を販売する場合は、ベンダにとって、個々のカード会社との契約等の煩わしい手間が省けるというメリットがある。

【0186】次に、ブラウザのヘルパ・アプリケーションを起動することにより、特定のパスワードを通知するオンライン通信サービスシステムについて述べる。このシステムでは、RISクライアント115をWWWブラウザ114にヘルパとして登録するとともに、ホームページ上にヘルパ起動のアンカーファイルを置く。

【0187】そして、ユーザーがこのアンカーファイルをクリックすると、RISクライアント115が自動的にRISサーバ112に接続する。RISサーバ112は、指定された通信サービスの課金処理を行い、ベンダに購入報告を行うとともに、ユーザーにサービス利用のためのパスワードを通告する。ユーザーは、このパスワードをWWWブラウザ114の画面に入力することで、そのサービスが受けられるようになる。

【0188】図16は、このようなオンライン通信サービスシステムを示している。通信サービスのベンダである占いの館161は、インターネット117上にホームページ162を開き、これを自社の占いサービスの受付画面とする（処理P21）。また、占いサービスの利用権を表す占いチケットとなるパスワード情報を、図51、52に示した方法で、ユーザーへの通告としてRISサーバ112に登録する（処理P21）。

【0189】ホームページ162のHTMLファイルは、図17のように記述される。これにより、占いチケ

ットに対応するRisアイコン163と、パスワードの入力欄164が表示される。Risアイコン163には、ヘルパ起動のためのアンカーファイル165（FTELL.RIS）がリファレンスとして設定されている。

【0190】このファイルFTELL.RISの[RIS]セクションには、図18に示すように、占いサービスのサービス名とソフトウェア番号（Soft）とが記述される。このソフトウェア番号は、サービスの識別番号として用いられる。

【0191】また、アンカーファイル165におけるWWWサーバのMIME設定は、上述のソフトウェア配達システムと同様にしておく。これにより、WWWブラウザ114がこのリファレンスを参照してきたとき、対応するWWWサーバはMIMEタイプとしてapplication/x-risを返すようになる。

【0192】ユーザー側は、上述のソフトウェア配達システムと同様に、RIS会員として既にユーザーID/パスワードおよびマシンID/パスワードが付与されているものとする。さらに、WWWブラウザ114に、RISクライアント115をヘルパ・アプリケーションとして登録しておく。

【0193】この状態で、ユーザーが占いの館ホームページ162にアクセスし（処理P22）、占いチケットの横のRisアイコン163をクリックしたとする（処理P23）。このとき、WWWブラウザ114は、RISクライアント115を起動し、RISクライアント115にファイルFTELL.RISの内容を渡す（処理P24）。

【0194】起動されたRISクライアント115は、RISサーバ112に接続し、暗号化されたパスワードでログインする。インターネット117上でのログインのシーケンスやRISクライアント115を使用するための設定は、図4、5、6に示した方法と同様である。

【0195】ログインの後、RISクライアント115は、ファイルFTELL.RISに記述されたソフトウェア番号をRISサーバ112に送り（処理P25）、RISサーバ112は、その番号により指定されるサービスの購入代金の課金処理を行い、その後、サービス購入者を識別するためのパスワードをユーザーへ通告する（処理P26）。

【0196】パスワードの通告は、RISセンターからユーザーへの連絡であり、例えば図19に示すような画面を、メッセージボックスの形式で端末113上に表示することに行われる。

【0197】ユーザーは、受け取ったパスワードをホームページ162上に表示された入力欄164に入力することで、対応するWWWサーバを通じて占いサービスを受けることができるようになる（処理P27）。このためには、占いサービスを提供するWWWサーバ側では、パス

ワード欄の値を得て、サービスの利用権を確認する機能を持っている。

【0198】この機能の実現方法としては、図17のHTMLファイルに記述されているCGI (common gateway interface) のスクリプトファイルura.cgiを利用する。ファイルura.cgiには、図20に示すようなサービス利用権の確認処理のロジックが記述される。

【0199】確認処理が開始されると、WWWサーバ上 のCGIプロセスは、まず入力されたパスワードの値を取得し（ステップS201）、それをRISサーバ112に登録したパスワードと比較して、正しいパスワードかどうかを確認する（ステップS202）。

【0200】パスワードが正しければ、そのユーザは課金されているものとみなし、有料の占いサービス提供画面を表示して（ステップS203）、処理を終了する。パスワードが正しくなければ、その誤りを指摘するメッセージをホームページ162上に表示して（ステップS204）、処理を終了する。

【0201】このような通信サービスにおけるパスワードの運用形態としては、すべてのユーザに共通のパスワードを与えて運用し続ける方法が考えられる。また、ユーザ間でのパスワードの漏洩またはパスワード推測による不正使用の防止するため、およびサービスの提供期間を限定するために、一定期間（数分、数時間、数日等）毎にパスワードを変更する方法やユーザ毎に異なるパスワードを発行する方法などもある。また、これらのパスワード保護方法を併せて用いることもできる。

【0202】さらに、RISサーバ112への登録時に、パスワードを固定した情報とするのではなく、特定の計算アルゴリズムを用いて、パスワードを動的に生成することも可能である。

【0203】以上の操作が行われると、RISサーバ112のデータベースには、図12、13と同様のサービス購入履歴が残る。そのサービス購入履歴を元に、上述のソフトウェア配送システムと同様の手順で、購入代金が決裁される（処理P28）。

【0204】このように、RISクライアント115をWWWブラウザ114から起動されるヘルパ・アプリケーションとして登録しておくことで、インターネット117上でのオンライン通信サービスシステムが実現される。また、RISクライアント115をWWWブラウザ114のプラグインとして登録しておくことも可能である。

【0205】図16のシステムでは、ユーザにパスワードを知らせることで通信サービスの利用権を与えているが、その代わりに、サービスを受けるためのURL (uniform resource locator) を通知することも考えられる。URLとは、ネットワーク上の資源を統一的に表現する識別情報である。

【0206】この場合、RISサーバ112は、課金処理後に、通信サービスのURLをユーザに通知する。そして、このURLは、課金を受けたものだけが知り得るように運用しておく。例えばURLを頻繁に変更すれば、ユーザは最新のURLを知るためにチケットを購入しなければならなくなる。

【0207】図21は、このような通信サービスシステムを示している。このシステムの動作は、基本的に図16のシステムと同様である。まず、占いの館161は、インターネット117上にホームページ166を開き、これを自社の占いサービスの受付画面とする（処理P31）。また、占いチケットとなるURL情報を、図51、52に示した方法で、RISサーバ112に登録する（処理P31）。

【0208】ホームページ166上には、占いチケットに対応するRisアイコン167と、“チケット購入で占いの部屋へのURLが表示されます”というメッセージが表示される。Risアイコン167には、ヘルパ起動のためのアンカーファイル165（図18のFTEL L.RIS）がリファレンスとして設定されている。

【0209】ユーザが占いの館ホームページ166にアクセスし（処理P32）、占いチケットの横のRisアイコン167をクリックしたとする（処理P33）。このとき、WWWブラウザ114は、RISクライアント115を起動し、RISクライアント115にファイルFTEL L.RISの内容を渡す（処理P34）。

【0210】起動されたRISクライアント115は、RISサーバ112に接続し、暗号化されたパスワードでログインし、ファイルFTEL L.RISに記述されたソフトウェア番号をRISサーバ112に送る（処理P35）。RISサーバ112は、その番号により指定されるサービスの購入代金の課金処理を行い、その後、占いサービスページ168のURLをユーザへ通告する（処理P36）。URLの通告は、例えば図19と同様のメッセージボックスを用いて行われる。

【0211】ユーザは、通告によって知り得た占いサービスへのURLをWWWブラウザ114上で指定することで、そのサービスページ168にアクセスして、占いサービスを受けることができるようになる（処理P37）。

【0212】また、図21のシステムにおいて、URLをユーザに通知する代わりに、そのURLを参照するブラウザを自動的に起動することも可能である。この場合、RISセンターからのURL通知をトリガとして、ソフトウェアによりブラウザを起動することで、ユーザがURLを直接扱うことなく、URLに対応したサービス画面へのアクセスが可能になる。

【0213】WWWブラウザ114の実装形態により、すでに起動されているWWWブラウザ114が、外部からのイベントによりURL指定を自動取得可能な場合

は、R I Sクライアント115は、WWWブラウザ114が読み込み可能な形式でURLをそれに通知する。このような方法としては、例えば、WWWブラウザ114の所定のファイルにURLを書き込んだ後、動作しているWWWブラウザ114にソフトウェアシグナルを送付する方法がある。

【0214】WIN95(Win dows 95)の場合、例えば図22に示すようなファイルWORK. URLを作成する。このファイルWORK. URLには、モザイク、NETSCAPE等のブラウザのタイプに応じて、R I Sサーバ112から通知されたURLが書き込まれる。

【0215】そして、R I Sクライアント115は、WIN95のAPI(application programming interface)を使用して、WWWブラウザ114を立ち上げる。APIとは、オペレーティングシステムが提供するプログラミング・インターフェースである。

【0216】この場合のAPIは、例えば“Shell Execute(~, “WORK. URL”, ~)”のように記述される。これにより、WWWブラウザ114は、ファイルWORK. URLから自動的にURLを取得して、対応するサービス画面にアクセスする。

【0217】また、WWWブラウザ114が、上述の方法で、ソフトウェア的にURL指定を自動取得可能でない場合は、所定のURLを初期URL引数として与えて、R I Sクライアント115から別途WWWブラウザ114を起動する。複数のWWWブラウザ114が同時に並行して動作すると不都合がある場合は、以前から動作していたWWWブラウザ114を一旦終了させ、その後で改めてWWWブラウザ114を起動すればよい。

【0218】次に、トランザクション用ヘルパとR I Sシステムとで構成するトランザクション処理システムについて述べる。このシステムでは、トランザクション用ヘルパを用意し、トランザクションの使用権をR I Sシステムに登録しておく。そして、ヘルパとして起動されたR I Sシステムが、トランザクション用の別のヘルパと連携することにより、トランザクション処理の使用権のデストリビューションと課金処理とを行う。

【0219】図23は、このようなトランザクション処理システムを示している。ベンダであるVOICE工房のWWWサーバ171は、例えば入力されたユーザの音声を元に占いを実行する音声占いのトランザクションサービスを提供する。まず、WWWサーバ171は、音声占いのホームページ172をインターネット117上に開き、そのトランザクションサービスの使用権を表す音声占い券を、ソフトウェアとしてR I Sサーバ112に登録する(処理P41)。

【0220】また、ユーザ端末113上では、WWWブラウザ114のヘルパとして、R I Sクライアント115とVoice処理プログラム178が登録される。V

oice処理プログラム178は、ユーザから音声の入力を受けて、各種フィルタリング処理の後、音声ファイルを作成する専用のソフトウェアであり、VOICE工房により作成/配布される。

【0221】ユーザは、まず、WWWブラウザ114からVOICE工房ホームページ172にアクセスし(処理P42)、音声占い券販売のアイコン173をクリックする(処理P43)。

【0222】このアイコン173には、R I Sクライアント115を起動するためのアンカーファイル176(URANA. R I S)がリファレンスとして設定されており、WWWブラウザ114は、R I Sクライアント115を起動して、ファイルURANA. R I Sの内容を渡す(処理P44)。ファイルURANA. R I SにおけるMIME設定は、図8のシステムと同様である。

【0223】起動されたR I Sクライアント115は、インターネット117を介してR I Sサーバ112に接続し(処理P45)、ダイレクトに音声占い券のデストリビューションを行う。

【0224】ここでは、デストリビューション処理として、R I Sクライアント115がVoice処理プログラム178の初期設定ファイル179(Voice. ini)の情報を書き換える(処理P46)。例えば、ファイルVoice. iniの[Permission]セクションに“YES”を書き込むことで、音声占い券のデストリビューションが行われ、ユーザにサービスの利用権が与えられる。

【0225】次に、ユーザがホームページ172の音声入力開始のアイコン174をクリックする(処理P47)。このアイコン174には、Voice処理プログラム178を起動するためのアンカーファイル177(KUBO. VOC)がリファレンスとして設定されており、WWWブラウザ114は、Voice処理プログラム178を起動する(処理P48)。アンカーファイル177におけるMIME設定として、ファイルタイプ“. VOC”がMIMEタイプ“application/x-voice”に対応付けられている。

【0226】起動されたVoice処理プログラム178は、図24に示すような処理を行う。Voice処理プログラム178は、まず、初期設定ファイル179の[Permission]セクションに“YES”と記述されているかどうかを調べる(ステップS211)。ここに“YES”と記述されていなければ、“占い券未購入”というメッセージを表示して(ステップS216)、処理を終了する。

【0227】ここに“YES”と記述されていれば、音声入力動作を開始し(ステップS212)、入力音声のフィルタリング等の各種ローカル処理を行って(ステップS213)、音声ファイル(不図示)を生成/出力する(ステップS214)。そして、ファイルVoice

41

e. iniの[Permission]セクションの“YES”を消去し(ステップS215)、処理を終了する。

【0228】こうして、音声ファイルが outputされると、ユーザは、次に占い開始のアイコン175をクリックし、占いサービスを実行する(処理P49)。占い開始のページは、例えば図25に示すように構成される。図25においては、音声ファイル名入力欄181、Browseアイコン182、ADDアイコン183、および実行アイコン184が表示されている。

【0229】Browseアイコン182がクリックされると、ファイルセレクタ185が開き、ここで選択された音声ファイル名が自動的に入力欄181に入力される。ADDアイコン183は、入力する音声ファイルを追加する際に用いられる。HTMLファイル186は、この占い開始ページの記述方法を表す。

【0230】ユーザにより音声ファイル名が入力され、実行アイコン184がクリックされると、指定された音声ファイルが占いサービスを行うWWWサーバ171に入力動作を開始し(ステップS223)、入力音声のアップロードされる。音声ファイルのアップロードは、既知のHTMLファイルアップロード機能を用いて行われる。WWWサーバ171は、アップロードされた音声ファイルを処理して、占い結果180をWWWブラウザ114に返す(処理P50)。

【0231】音声占いの使用料金は、RISクライアント115がRISサーバ112に接続した時点で課金処理され、その後、RISサーバ112からVOICE工房に払い戻される(処理P51)。

【0232】ところで、上述の初期設定ファイル179を利用して、ローカルなトランザクション処理プログラムから直接RISクライアント115を起動し、図23と同様の方法でトランザクション処理の使用権のデストリビューションと課金処理とを行うこともできる。

【0233】この場合、トランザクション処理プログラムを、図26のフローチャートに示すように構成する。トランザクション処理プログラムは、まず、ファイルvoice.iniの[Permission]セクションに、サービス使用権の購入処理中であることを示す情報“BUYING”が書き込まれているかどうかを調べる(ステップS221)。

【0234】ここに“BUYING”が書かれていれば、それが消去されるまで同じ判定を繰り返し、“BUYING”が書かれていなければ、次に、その[Permission]セクションに、購入済を表す情報“YES”が書き込まれているかどうかを調べる(ステップS222)。

【0235】ここに“YES”が書かれていなければ、サービス使用権(占い券)を購入中でも購入済でもないことがわかる。そこで、トランザクション処理プログラムは、占い券を購入するかどうかをユーザに問い合わせる

42

(ステップS228)。ここで、ユーザが占い券の購入を選択しなければそのまま処理を終了する。

【0236】ユーザが占い券の購入を選択すると、トランザクション処理プログラムは、ファイルvoice.iniの[Permission]セクションに“BUYING”を書き込んで(ステップS229)、RISクライアント115を起動し(ステップS230)、ステップS228以降の処理を繰り返す。

【0237】起動されたRISクライアント115は、図23のシステムと同様の方法でRISサーバ112に接続して、占い券を購入する。占い券の購入が終わると、RISクライアント115は、ファイルvoice.iniの[Permission]セクションの“BUYING”を消去して、代わりに“YES”を書き込む。

【0238】このとき、ステップS221の判定結果がNOとなり、ステップS222の判定結果がYESとなる。そこで、トランザクション処理プログラムは、音声入力動作を開始し(ステップS223)、入力音声のファイルタリング等の処理を行って(ステップS224)、占いを実行する(ステップS225)。

【0239】そして、占い結果を表示し(ステップS226)、ファイルvoice.iniの[Permission]セクションの“YES”を消去して(ステップS227)、処理を終了する。[Permission]セクションの“YES”を消去することで、トランザクション処理は初期状態を回復する。

【0240】このように、RISシステムと連携するトランザクション処理プログラムをユーザ端末113上に備えることで、WWWブラウザ114の介在なしにRISシステムを利用することが可能になる。

【0241】また、図23のトランザクションサービスシステムにおいて、複数回のサービス利用権を販売することもできる。この場合は、RISサーバ112には複数回の使用権を登録しておき、Voice処理プログラム178側では、トランザクション処理毎に、初期設定ファイルのカウント数を1だけデクリメントする構成を用いる。

【0242】図27は、このようなトランザクションサービスシステムを示している。図27のシステムにおいては、RISサーバ112には、1回、5回、10回の3種類の占い券が、それぞれ、ソフトウェア番号160、161、162に対応して登録されている。そして、ベンダのVOICE工房ホームページ191には、音声占い券販売のアイコンとして、1回券、5回券、10回券のアイコン192、193、194が表示される。

【0243】これらのアイコン192、193、194には、それぞれ、アンカーファイル195(URAN A.RIS)、196(URANA2.RIS)、19

43

7 (URANA3. RIS) がリファレンスとして設定されている。そして、ファイルURANA. RISにはソフトウェア番号160が記述され、ファイルURANA2. RISにはソフトウェア番号161が記述され、ファイルURANA3. RISにはソフトウェア番号162が記述されている。

【0244】ユーザがいずれかの占い券を選択して、対応するアイコンをクリックすると、RISクライアント115は、そのアイコンにリンクしているアンカーファイルのソフトウェア番号をRISサーバ112に送り、初期設定ファイル179の[Permission]セクションに、対応するカウント数(Count)を書き込む。例えば、10回券が購入された場合は、Count=10となる。これにより、複数回のサービス利用権がユーザ端末113に設定される。

【0245】図28は、このシステムにおけるVoice処理プログラム178の処理のフローチャートである。Voice処理プログラム178は、まず、初期設定ファイル179の[Permission]セクションのCountの値が0かどうかを調べる(ステップS231)。Countが0であれば、“占い券未購入”というメッセージを表示して(ステップS236)、処理を終了する。

【0246】Countが0より大きければ、音声入力動作を開始し(ステップS232)、入力音声のフィルタリング等の各種ローカル処理を行って(ステップS233)、音声ファイルを生成／出力する(ステップS234)。そして、ファイルVoice.iniの[Permission]セクションのCountの値を、1だけデクリメントして(ステップS235)、処理を終了する。

【0247】このようなVoice処理プログラム178を用いれば、ユーザは、購入したサービス利用権の利用回数だけ、サービスを受けることができる。図27のシステムにおけるその他の設定および動作は、図23のシステムと同様である。

【0248】次に、ローカルなトランザクション処理プログラムとRISシステムの連携処理により、データの取得および課金を行うシステムについて述べる。このシステムでは、トランザクション処理プログラムから直接RISクライアント115を起動し、図23と同様の方法でトランザクション処理用のデータを入手する。

【0249】例えば、トランザクション処理プログラムが競馬予想ソフトウェアである場合、その処理のフローチャートは、図29に示すようになる。競馬予想ソフトウェアは、起動時に、まず新しいデータを取得するかどうかをユーザに問い合わせる(ステップS241)。

【0250】そして、ユーザが新しいデータを取得しない意思決定を行った場合は、既存の競馬データを用いて予想を実行し(ステップS243)、処理を終了する。

44

また、ユーザが新しいデータを取得する意思決定を行った場合は、RISクライアント115を起動する(ステップS242)。

【0251】RISクライアント115は、ソフトウェア番号を元にしてRISサーバ112にアクセスする。RISサーバ112には、図30に示すように、競馬データがあらかじめ登録されており、図8と同様な方法で、ダイレクトに競馬データのデストリビューションを行う。そして、競馬予想ソフトウェアは、配送された競馬データを用いて予想を実行し(ステップS243)、処理を終了する。

【0252】図31は、RISクライアント115とRISサーバ112による競馬データのデストリビューション処理を示している。この処理は、図44、45、46に示した方法を利用して実行される。まず、RISクライアント115が、競馬予想ソフトウェアに付随する競馬データファイルKEIBA.DATの日付を調べ、RISサーバ112に送る(ステップS251)。ファイルKEIBA.DATには、例えば図32に示すように、競走馬等のデータA、B、Cが格納されている。

【0253】RISサーバ112は、図33に示すような日付・ファイル名対応表を参照して、送られた日付に対応するファイル名を検索し、それに対応するファイルを、追加データファイルとしてRISクライアント115に送付する(ステップS252)。そして、その内容をファイルKEIBA.DATに追加して、ファイルKEIBA.DATを更新し(ステップS253)、処理を終了する。

【0254】図33の日付・ファイル名対応表は、あらかじめRISサーバ112に登録されており、必要に応じて更新される。日付・ファイル名対応表に記載されたファイルFILE1.LZH、FILE2.LZH、FILE3.LZHには、図24に示すようなデータの組み合わせが含まれる。

【0255】例えば、ファイルFILE1.LZHにはデータD、E、F、Gが含まれ、ファイルFILE2.LZHにはデータE、F、Gが含まれ、ファイルFILE3.LZHにはデータF、Gが含まれている。このように、ファイル毎にデータの組み合わせを変えておくことで、日付の古いファイルKEIBA.DATほど、多くの追加データが与えられるようにすることができる。

【0256】図29のようなトランザクション処理プログラムによれば、WWWブラウザ114の介在なしに、RISシステムを利用してサービスに必要なデータを配送することができる。

【0257】また、トランザクション処理プログラムが、起動時にデータファイルの日付を見て、前回のデータ更新時から一定時間経過している場合のみ、RISサーバ112に接続し、データ取得を行う構成にすることもできる。この場合、トランザクション処理プログラム

45

は、現在の日付がデータファイルの日付より所定日数以上経過していれば、R I Sサーバ112に接続して、最新のデータによりデータファイルを更新する。

【0258】図35は、このような競馬予想ソフトウェアのフローチャートである。競馬予想ソフトウェアは、起動時に、現在の日付とデータファイルKEIBA.DATの日付の差を計算し、それが2ヶ月を越えているかどうかを判定する(ステップS261)。

【0259】その差が2ヶ月を越えていなければ、既存の競馬データを用いて予想を実行し(ステップS26

3)、処理を終了する。また、その差が2ヶ月を越えていれば、R I Sクライアント115を起動し、新しい競馬データをR I Sサーバ112から取得する(ステップS262)。そして、配達された競馬データにより更新されたファイルKEIBA.DATを用いて、予想を実行し(ステップS263)、処理を終了する。

【0260】次に、複数のR I Sサーバが存在するネットワーク環境において、ユーザ端末(クライアントマシン)のマシンID(M I D)にサーバ識別子を混ぜることで、サーバによるユーザ端末の誤認識を防ぐR I Sシステムについて述べる。

【0261】このシステムでは、サーバ識別子とクライアントマシンの識別子を合成して、そのクライアントマシンを識別するM I Dを生成する。そして、サーバはクライアントから送られたM I Dをサーバ部とクライアント部に分解し、サーバ部がそのサーバの識別子と異なっていたら、クライアントとの接続を切断する。

【0262】従来のR I Sシステムによるクライアント識別の方法は、サーバがただ1つしか存在しないことを前提としていた。これに対して、本実施形態の方法を用いれば、複数のサーバがサービスを行い、1つのクライアントが各サーバに接続する場合でも、サーバによるクライアントの誤認識を防ぐことができる。

【0263】このシステムでは、それぞれ異なる複数のサーバは、それ自身を表す固有の識別子を有し、クライアントのM I Dは、常にアクセス先のサーバ識別子を用いて作成することにする。したがって、同じマシンでも、そのアクセス先によってM I Dが異なってくる。

【0264】図36は、サーバA、Bとクライアントマシン $\alpha$ 、 $\beta$ を含むシステムを示している。このシステムにおいて、サーバAは、クライアント番号1に対してマシン $\alpha$ の情報(ディレクトリ情報やメモリ量等)を保持し、クライアント番号2に対してマシン $\beta$ の情報を保持する。また、他のサーバBは、クライアント番号2に対してマシン $\alpha$ の情報を保持し、クライアント番号1に対してマシン $\beta$ の情報を保持している。

【0265】図48に示した従来の方法では、クライアント番号自体がM I Dとして使われていた。この方法をそのまま図36のシステムに適用すると、マシン $\alpha$ がクライアント番号1をM I DとしてサーバBに接続した場

46

合、サーバはそれをマシン $\beta$ のM I Dとみなして、マシン $\alpha$ から送られる情報をマシン $\beta$ の情報に上書きしてしまう事故が発生し得た。

【0266】しかし、クライアント識別子にサーバ識別子を混ぜてM I Dを生成することで、クライアントが誤った識別子を用いてサーバに接続した場合に、サーバ側でこれをチェックして、誤りを検出することが可能になる。これにより、サーバは、マシン情報を誤って上書きしてしまうことを避けるとともに、クライアントに対して、誤りを通知することができる。

【0267】例えば、マシン $\alpha$ がサーバA、Bにアクセスする際のM I Dを、それぞれ“A 1”、“B 2”とし、マシン $\beta$ がサーバA、Bにアクセスする際のM I Dを、それぞれ“A 2”、“B 1”とする。

【0268】このとき、マシン $\alpha$ が、誤って“B 2”をM I DとしてサーバAにアクセスした場合、サーバAは、まず、そのM I Dをサーバ部“B”とクライアント部“2”とに分解して、サーバ部の識別子を調べる。この場合、サーバ部“B”が自身の識別子と異なるので、このアクセスは誤りと判断し、マシン $\alpha$ との接続を切断する。

【0269】また、マシン $\alpha$ が、誤って“A 1”をM I DとしてサーバBにアクセスした場合も、同様にして誤りが検出され、マシン $\alpha$ との接続が切断される。ここでは、アクセスの誤りを接続の切断という方法でクライアントに通知しているが、代わりにエラーメッセージ等を用いてもよい。

【0270】このシステムのサーバ識別子としては、ドメイン名r i s . g m s n e t . o r . j pのように、世界で唯一であることが保証されているものを用いることが望ましい。そうすれば、サーバ識別子の重複という事故を避けることができるので、クライアントの識別を完璧に行うことができる。したがって、1つのクライアントで複数のサーバを使い分ける場合でも、クライアントのマシン情報が混乱することが避けられる。

【0271】また、このような複数のサーバの取扱いにおいて、各サーバに対応する初期設定ファイルをクライアント側に持つことも考えられる。この場合、基本となるサーバの初期設定ファイルに、他のサーバの初期設定ファイルがあるかどうかを、拡張情報として記述しておく。

【0272】例えば、図37に示すファイルR I S . I N Iを基本の初期設定ファイルとし、図38に示すファイルR I S 2 . I N Iを別のサーバの初期設定ファイルとする。このように、サーバ毎に異なる初期設定ファイルを用意すれば、矢印で示されるように、それぞれまったく異なるユーザID/パスワードおよびM I Dを扱うことができる。

【0273】また、図37のファイルR I S . I N Iの中には【EXTENSION】セクションが設けられ、

10

20

30

40

40

50

ここに他の初期設定ファイルをアクティブにするかどうかを記述できる。ここでは、ファイルRIS.1NIとRIS2.1NIがアクティブ(ON)になっており、動作時には、他のファイルRIS2.1NIも自動的に参照される。

【0274】図36に示した方法を用いれば、サーバ側は正しくクライアントマシンの情報をハンドリングすることができる。次に問題となるのは、クライアント側にとって、正しいサーバに接続できたかどうかを確認することにある。というのは、複数のサーバが存在する場合、間違って悪意のあるサーバに接続するかもしれないという危険性があるからである。

【0275】そこで、次に、正しいサーバを識別するRISシステムについて述べる。このシステムでは、RSA(Rivest-Shamir-Adleman)暗号による電子署名の機能を用いたログインセッションを設ける。RSA暗号は、非対称な暗号システムであり、暗号化と復号化にはそれぞれ異なる鍵情報が用いられる。

【0276】このログインセッションにおいて、サーバは、決められた情報を秘密鍵で暗号化してクライアントに送り、クライアントは、それを公開鍵で復号化することにより、サーバの認証を行う。これにより、クライアントは、ログイン先が正しいサーバかどうかを判定することができる。

【0277】図39は、このようなサーバ識別システムを示している。図39において、各サーバは、RSAの秘密鍵を保持し、対応する公開鍵をホームページ201に登録しておく。サーバのリストを表示するホームページ201が信用できるかどうかは、ユーザが判断するものとする。あるいは、信用できるホームページ201のURLをあらかじめクライアントに埋め込んでおいてよい。

【0278】サーバは、クライアントから接続時に任意の情報を平文で渡してもらい、それを秘密鍵で暗号化して返すと、クライアントは、サーバの公開鍵で元の平文を正しく復元することができる。正しく復元できたということは、サーバがその公開鍵と対を成す秘密鍵を保持していることになるので、正しいサーバであると判断できる。

【0279】図39において、マシンαは、サーバAへの接続に先立ち、その識別子“A”、公開鍵“公A”等のサーバ情報をホームページ201から取得し、MID“A1”を作成する。このとき、必要であれば、他のサーバの情報をも取得しておく。

【0280】この状態で、マシンαがサーバAを識別するログインシーケンスは、図40に示すようになる。マシンαがサーバAに接続すると、サーバAはサーバ識別のための情報(Word)を問い合わせてくる。そこで、マシンαが情報“apple”を平文で送ると、サーバAはそれを秘密鍵“秘A”で暗号化し、暗(a pp l e,

e, 秘A)として送り返す。

【0281】マシンαは、暗(a pp l e, 秘A)を公開鍵“公A”で復号化し、情報“apple”を取り出す。この情報は、先に送った情報と一致するので、接続先は正しいサーバAであると判断する。そこで、ユーザがUIDを入力し、マシンαは通常のログインシーケンスに移行する。

【0282】これに対して、サーバAになりましたサーバA'に対するログインシーケンスは、図41に示すようになる。マシンαがサーバA'に接続して、サーバA'に情報“apple”を送るところまでは、図40と同様である。サーバAは、受け取った情報を、適当に設定した秘密鍵“秘A'”で暗号化し、暗(a pp l e, 秘A')として送り返す。

【0283】ところが、マシンαが暗(a pp l e, 秘A')を公開鍵“公A”で復号化すると、平文“b q q m f”が取り出される。この情報は、先に送った情報と異なるので、接続先は正しいサーバAではないと判断し、接続を切断する。こうして、偽のサーバA'を識別することができる。

【0284】また、図40、41のシーケンスとは異なり、クライアントがサーバの公開鍵で暗号化した情報をサーバに送り、サーバがそれを秘密鍵で復号化して、クライアントに平文として送り返しても、同様の効果が得られる。この場合、クライアントは、サーバから送り返された平文が正しければ、そのサーバを正しいサーバと認識する。

【0285】図39のサーバ識別システムにおいて、サーバ認証鍵となる公開鍵および秘密鍵を固定したまま運用を続けると、いつか暗号を破られる可能性がある。そこで、これらのを定期的に更新することにより、暗号の安全性を高める必要がある。しかし、公開鍵が変更される度に、クライアント側のサーバ情報を設定し直すのは不便なので、この過程を自動化し、クライアントがサーバにログインするときに、毎回サーバ情報を取得するようとする。

【0286】そして、図8に示した方法を利用して、ホームページからRISクライアント115を起動する。この場合、RISアイコンにリンクしたアンカーファイルは、図42に示すように拡張され、その[SERVER]セクションにサーバ識別子が記述され、[OKEY]セクションに公開鍵が記述される。

【0287】WWWブラウザ114から起動されたRISクライアント115は、RISサーバに接続する前に、図43に示すような処理を行う。RISクライアント115は、まず、図42のアンカーファイルRIS2.RISの[SERVER]セクションを見て、RISサーバ“0002”へのアクセス権があるかどうかを調べる(ステップS271)。

【0288】ここに、サーバ識別子“0002”が記述

されていればアクセス権があると判断し、次に、[OK E Y] セクションを見て、新たな公開鍵 “1 2 3 4” を取り込む（ステップS272）。そして、[R I S] セクションを見て、ソフトウェア番号ではなく、“S t a r t=m e n u” と記述されていることを知る。そこで、ソフトウェアを要求するのではなく、初期メニューから R I S サーバ “0 0 0 2” にアクセスすることを認識し（ステップS273）、処理を終了する。

【0289】ステップS271において、サーバ “0 0 0 2” へのアクセス権がないことがわかると、エラー表示等の処理を行って（ステップS274）、処理を終了する。こうして、ファイル R I S 2. R I S の読み取りが終了すると、R I S クライアント 1 1 5 は、図40に示したようなログインセッションを開始する。

【0290】以上説明した実施形態において、暗号アルゴリズムは D E S と R S A に限られず、他の任意のものを用いることができる。また、図14のオンラインショッピングシステムでは、タオルセット、ハンカチーフ以外の任意の商品、サービスを販売することができ、図16、21の通信サービスシステムでは、占いサービス以外の任意の通信サービスを提供することができる。また、図23、27のトランザクションサービスシステムでは、音声占いサービス以外の任意のトランザクションサービスを提供することができる。

#### 【0291】

【発明の効果】本発明によれば、インターネット上でリモートインストールシステムを利用して、ソフトウェア配送サービス、オンラインショッピング、通信サービス、トランザクションサービス等の様々な会員制サービスを提供することが可能になる。また、インターネット上で接続先の認証や、パスワード、コンテンツ等の暗号化も行われ、サービスの安全性が保証される。

#### 【図面の簡単な説明】

【図1】本発明のサービスシステムの原理図である。

【図2】実施形態のシステム構成図である。

【図3】情報処理装置の構成図である。

【図4】サインアップシーケンスを示す図である。

【図5】第1の初期設定ファイルを示す図である。

【図6】第1のログインシーケンスを示す図である。

【図7】暗号化されたコンテンツの配送を示す図である。

【図8】インターネット上のソフトウェア配送システムを示す図である。

【図9】ソフト工房ホームページのHTMLファイルを示す図である。

【図10】第1のアンカーファイルを示す図である。

【図11】ソフトウェアの配送を示す図である。

【図12】購入テーブルを示す図である。

【図13】支払いテーブルを示す図である。

【図14】オンラインショッピングシステムを示す図で

ある。

【図15】受付票／購入通知送付処理を示す図である。

【図16】オンライン通信サービスシステムを示す図である。

【図17】占いの館ホームページのHTMLファイルを示す図である。

【図18】第2のアンカーファイルを示す図である。

【図19】パスワードの表示画面を示す図である。

【図20】サービス利用権の確認処理のフローチャートである。

【図21】URLを通知する通信サービスシステムを示す図である。

【図22】URL格納ファイルを示す図である。

【図23】第1のトランザクションサービスシステムを示す図である。

【図24】第1のV o i c e 処理プログラムのフローチャートである。

【図25】占い開始画面を示す図である。

【図26】トランザクション処理プログラムのフローチャートである。

【図27】第2のトランザクションサービスシステムを示す図である。

【図28】第2のV o i c e 処理プログラムのフローチャートである。

【図29】第1の競馬予想処理のフローチャートである。

【図30】R I S サーバの情報を示す図である。

【図31】データのデストリビューション処理のフローチャートである。

【図32】競馬データファイルを示す図である。  
【図33】日付・ファイル名対応表を示す図である。  
【図34】各ファイルに含まれるデータを示す図である。

【図35】第2の競馬予想処理のフローチャートである。

【図36】複数のサーバが存在するシステムを示す図である。

【図37】第2の初期設定ファイルを示す図である。

【図38】第3の初期設定ファイルを示す図である。

【図39】サーバ識別システムを示す図である。  
【図40】第2のログインシーケンスを示す図である。  
【図41】第3のログインシーケンスを示す図である。  
【図42】第3のアンカーファイルを示す図である。  
【図43】クライアントの処理のフローチャートである。

【図44】リモートインストールのフローチャート（その1）である。

【図45】リモートインストールのフローチャート（その2）である。

【図46】リモートインストールのフローチャート（そ

の3)である。

【図47】ユーザID登録のフローチャートである。

【図48】端末ID登録のフローチャートである。

【図49】販売のフローチャートである。

【図50】端末パスワードチェックのフローチャートである。

【図51】場の構成を示す図である。

【図52】作者の作業のフローチャートである。

【図53】オリジナルクラブ管理者の作業のフローチャートである。

【図54】転載先クラブ管理者の作業のフローチャートである。

【図55】アップロードを示す図である。

【図56】シェアウェア手続きを示す図(その1)である。

【図57】シェアウェア手続きを示す図(その2)である。

【図58】シェアウェア手続きを示す図(その3)である。

【図59】シェアウェア手続きを示す図(その4)である。

【図60】代金引き落とし手続きを示す図(その1)である。

【図61】代金引き落とし手続きを示す図(その2)である。

【図62】代金引き落とし手続きを示す図(その3)である。

#### 【符号の説明】

1、2 環境ファイル

3、4 キーテーブル

5 チェックスクリプト

6 ファイル本体

7 インストールスクリプト

11、12、13、14 クラブ

15 ソフトウェア

21 CFGファイル

22 説明ファイル

23 インストール関連ファイル

24 本体ファイル

25 定義ファイル

26 CHKファイル

27 書換えファイル

28 コンテンツデータベース

29 メニュー

30 ダイアログボックス

31 メッセージ

80 登録手段

81 キー情報付与手段

82 暗号化手段

83 リモートインストール手段

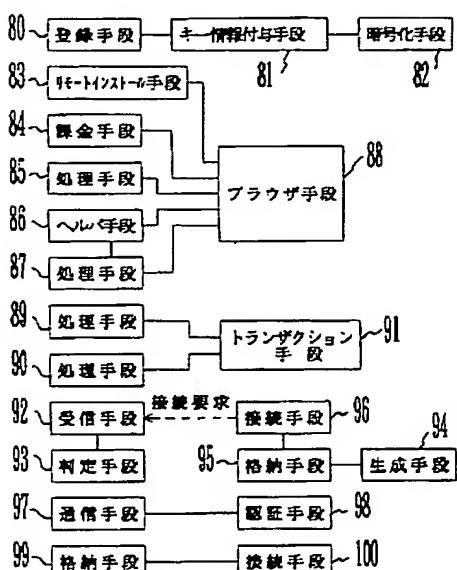
84	課金手段
85、87、89、90	処理手段
86	ヘルパ手段
88	ブラウザ手段
91	トランザクション手段
92	受信手段
93	判定手段
94	生成手段 94
95、99	格納手段
10 96、100	接続手段
97	通信手段
98	認証手段
11 1	ホスト計算機
11 2	RISサーバ
11 3	ユーザ端末
11 4	WWWブラウザ
11 5	RISクライアント
11 6	FENICS回線
11 7	インターネット
20 12 1	CPU
12 2	メモリ
12 3	入力装置
12 4	出力装置
12 5	外部記憶装置
12 6	媒体駆動装置
12 7	ネットワーク接続装置
12 8	バス
12 9	可搬記録媒体
13 0	データベース
30 13 1	秘密キーデータベース
13 2、179	初期設定ファイル
13 3	Challenge発生関数
13 4	合成関数
13 5	暗号化プログラム
13 6	復号化プログラム
14 1	ソフト工房
14 2	ソフト工房ホームページ
14 3、153、163、167、192、193、194	Risアイコン
40 14 4、154、165、176、177、195、196、197	アンカーファイル
15 1	α商店
15 2	α商店ホームページ
16 1	占いの館
16 2、166	占いの館ホームページ
16 4	パスワード入力欄
16 8	占いサービスページ
17 1	VOICE工房サーバ
17 2、191	VOICE工房ホームページ
50 17 3、174、175、182、183、184	ア

53

- イコン  
178 Voice処理プログラム  
180 占い結果  
181 音声ファイル名入力欄

【図1】

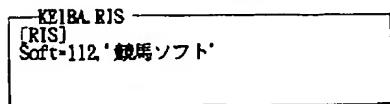
## 本発明の原理図



【図10】

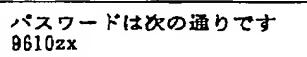
## 第1のアンカーファイルを示す図

144



【図19】

## パスワードの表示画面を示す図

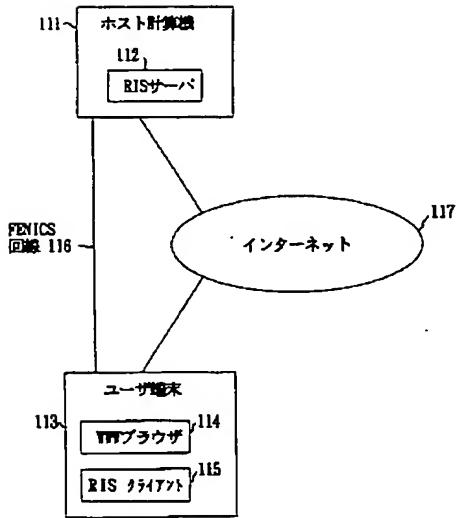


54

- 185 ファイルセレクタ  
186 HTMLファイル  
201 信用できるホームページ

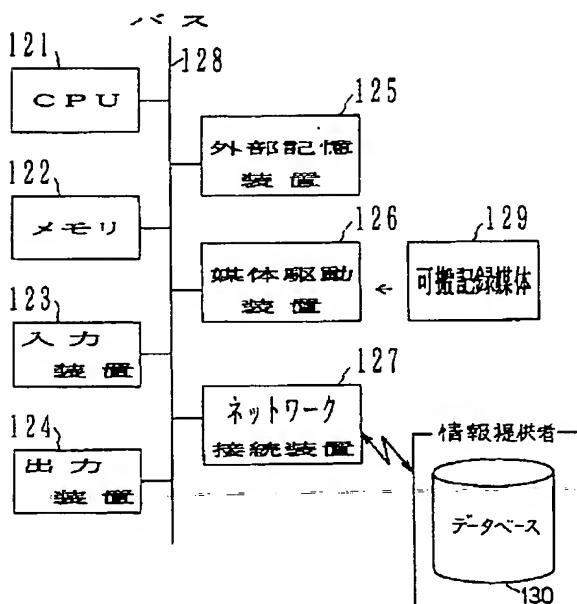
【図2】

## システム構成図



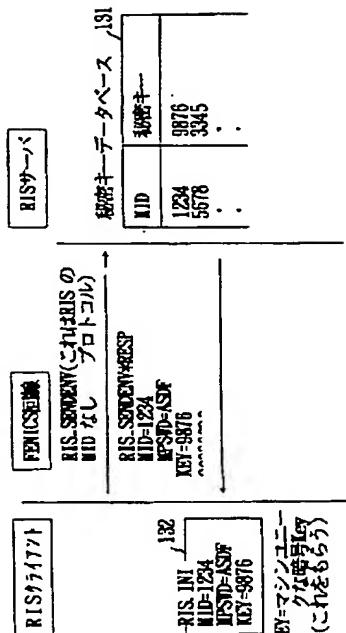
【図3】

## 情報処理装置の構成図



【図4】

ライソアップシケンスを示す図



【図7】

【図5】

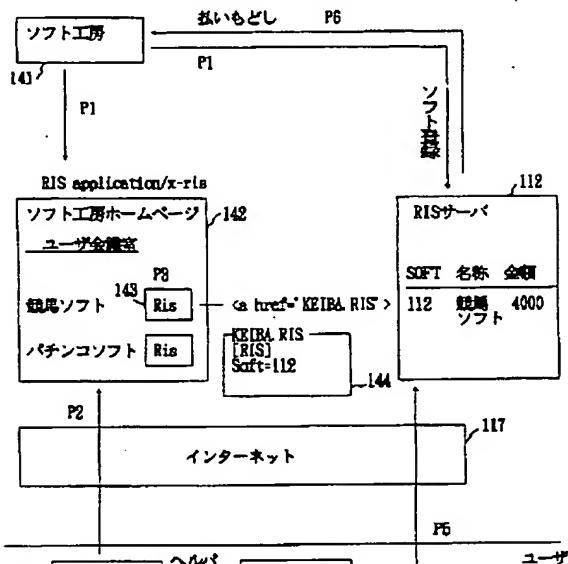
第1の初期設定ファイルを示す図

132

RIS.INI  
[INET]  
HOST=ris.gmoet.or.jp \*アドレス(ドメイン名)  
PORT=5021

【図8】

インターネット上のソフトウェア配達システムを示す図

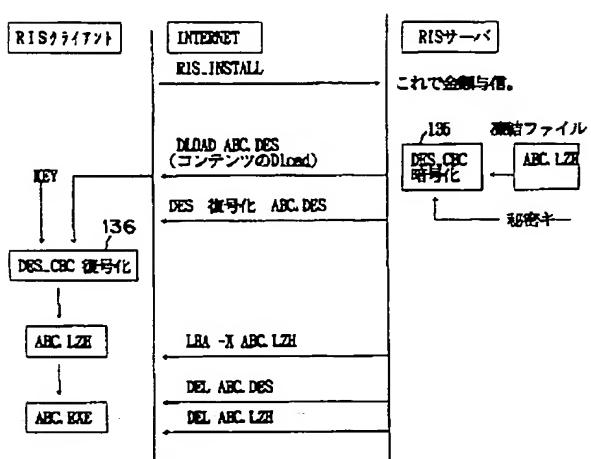


【図12】

購入テーブルを示す図

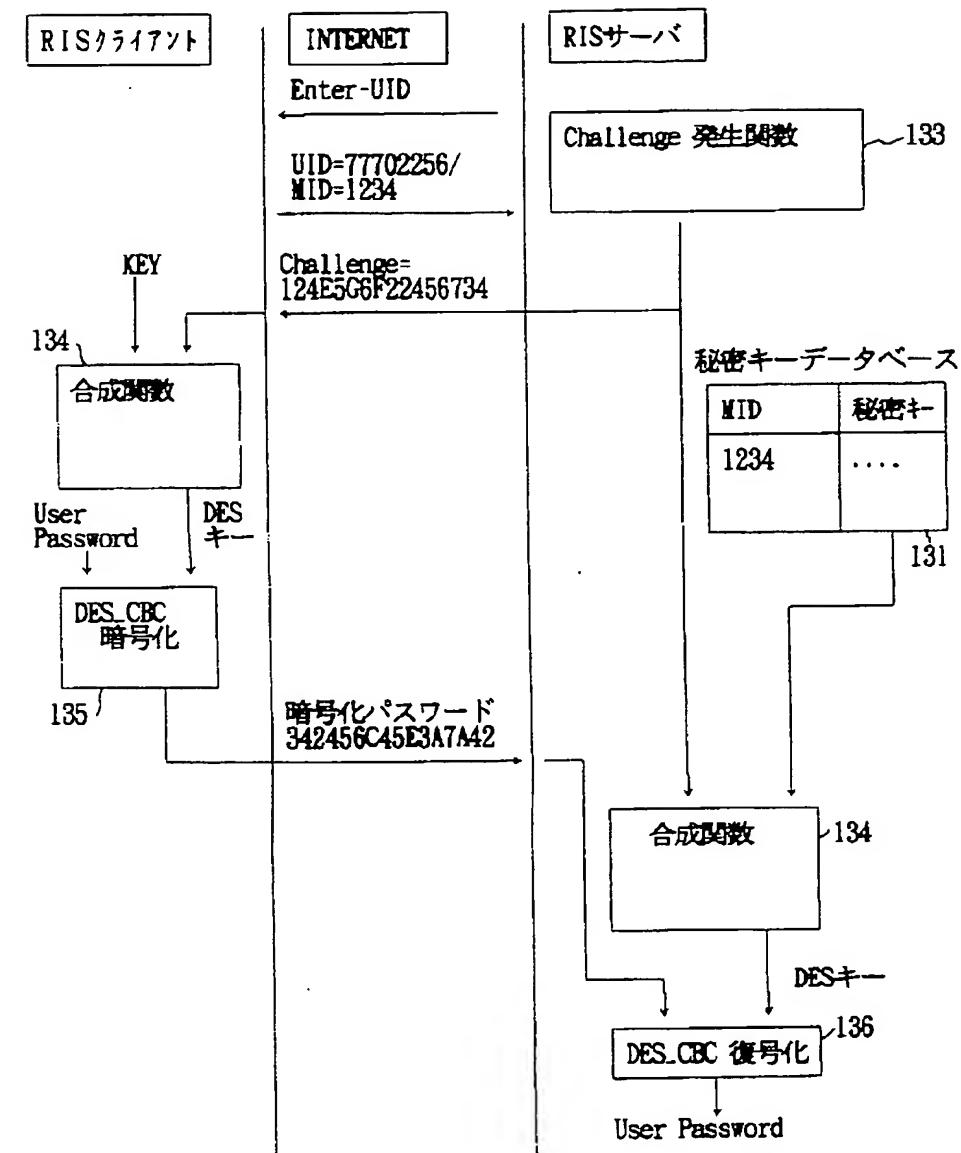
UID	Soft	品目	数量	単価	日付	Card.typ	Card.No
77702256	112	競馬ソフト	1	4000	96.10.25	JCB	

暗号化されたコンテンツの配達を示す図



【図6】

## 第1のログインシーケンスを示す図



【図13】

## 支払いデータルを示す図

消費者UID	ベンダUID	品目	単価	数量	日付
77702256	1234567	競馬ソフト	4000	1	98.10.25

【図9】

【図18】

ソフト工房ホームページのHTMLファイルを示す図 第2のアンカーファイルを示す図

165

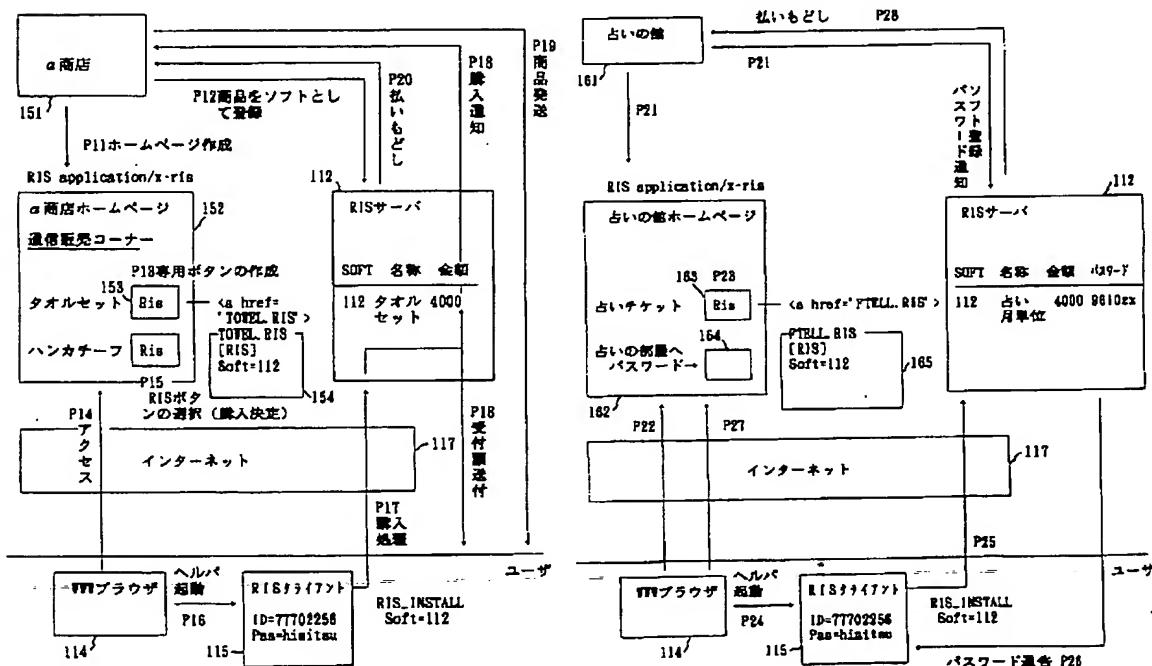
```
<html>
<head>
<title> ソフト工房HomePage</title>
</head>
<body>
~
<b>競馬ソフト.. 楽しい競馬</b>
<a href='KEIBA.RIS'>
<Image src='RISICON.JIF'></a>
<b>パチンコソフト... 楽しいパチンコ</b>
<a href='PACHI.RIS'>
<Image src='RISICON.JIF'></a>
~
</body>
</html>
```

FTELL.RIS  
[RIS]  
Soft=112. \*占い月単位\*

【図14】

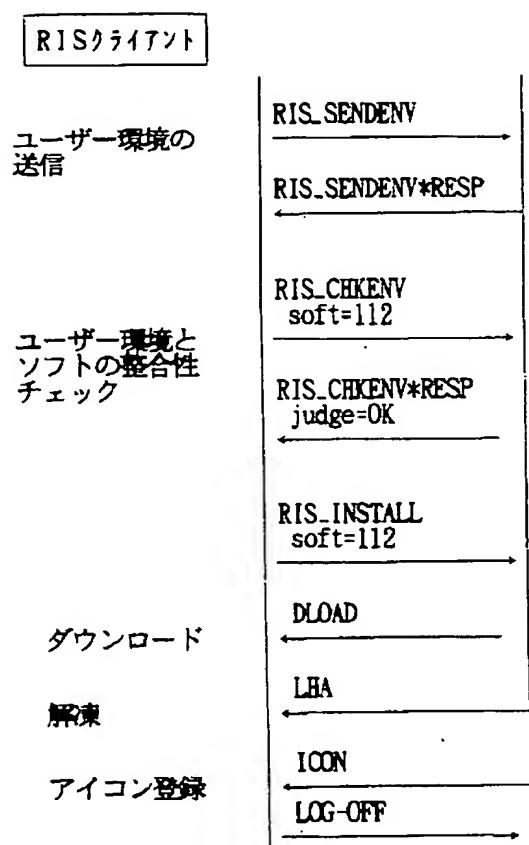
【図16】

オンラインショッピングシステムを示す図 オンライン通信サービスシステムを示す図



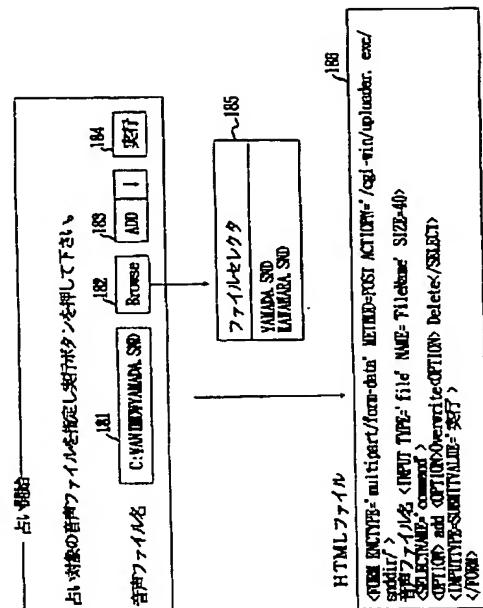
[図 1 1 ]

## ソフトウェアの配達を示す図



〔図25〕

### 占い開始画面を示す図

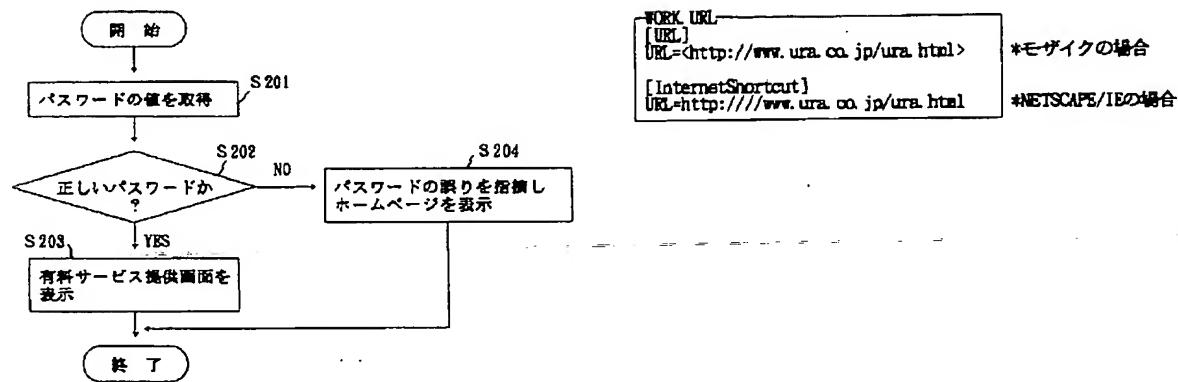


【四二〇】

## サービス利用権の確認処理のフローチャート

[図22]

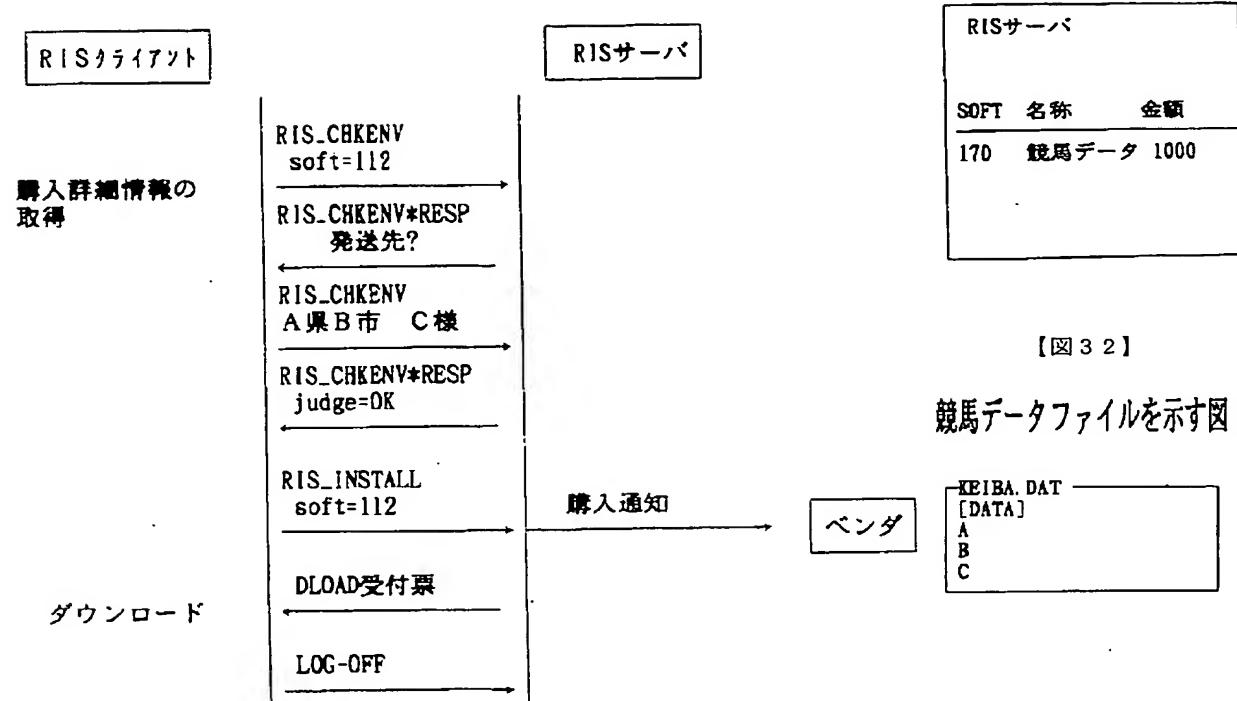
## URL格納ファイルを示す図



【図15】

【図30】

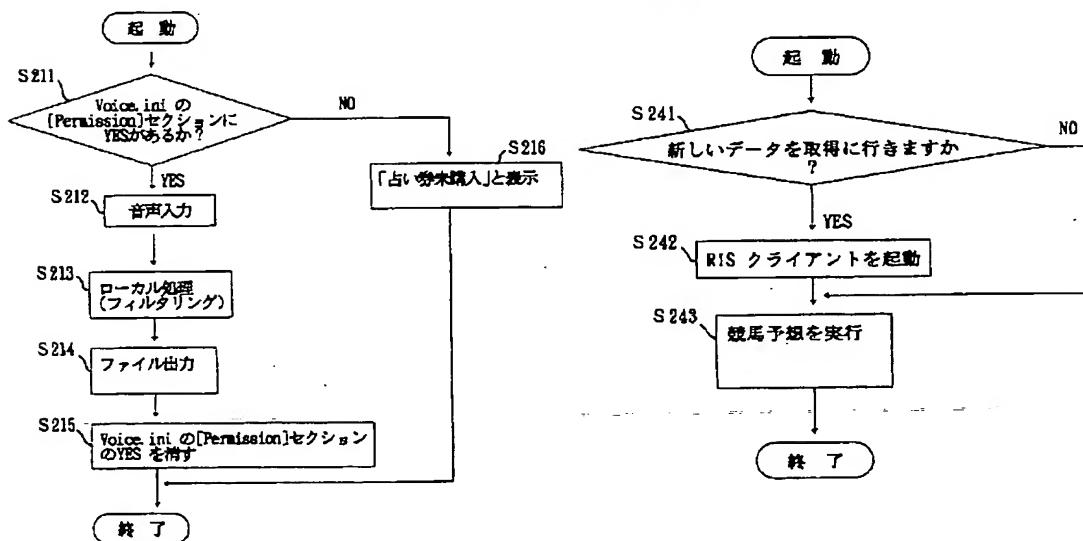
受付票 / 購入通知送付処理を示す図 RISサーバの情報を示す図



【図24】

【図29】

第1のVoice処理プログラムのフローチャート 第1の競馬予想処理のフローチャート



【図17】

占いの館ホームページのHTMLファイルを示す図 日付・ファイル名  
対応表を示す図

```

<html>
<head>
<title> 占いの館HomePage</title>
</head>
<body>
~
<b>
占いチケット</b>
<a href='FTELL.RIS'>
<Image src='ticket.JIF'></a>
<b>
占いの部屋へ</b>
<form method=GET action='http://www.ura.co.jp/ura.cgi'>
パスワード→<br>      <input name=password><br>
</form> <Image src='inftell.JIF'></a>
~
</body>
</html>

```

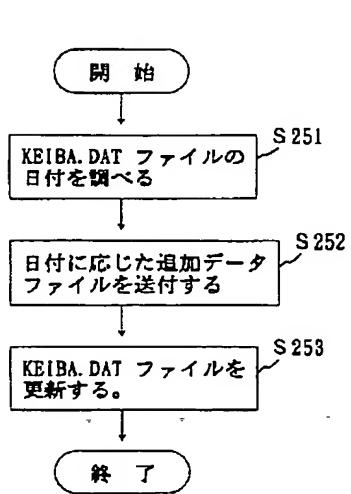
96.4.1	FILE1.LZH
96.6.1	FILE2.LZH
96.8.1	FILE3.LZH

【図31】

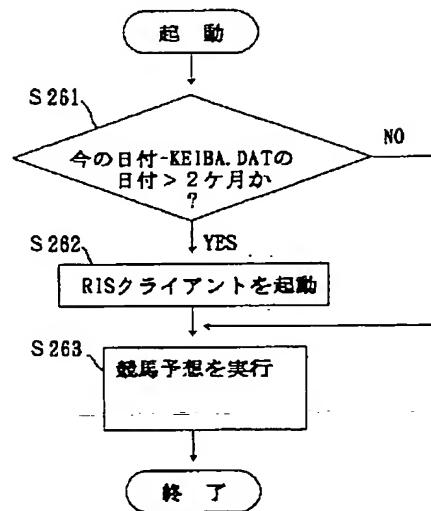
【図34】

【図35】

データのテストリビューション 各ファイルに含まれるデータを示す図 第2の競馬予想処理のフローチャート  
処理のフローチャート

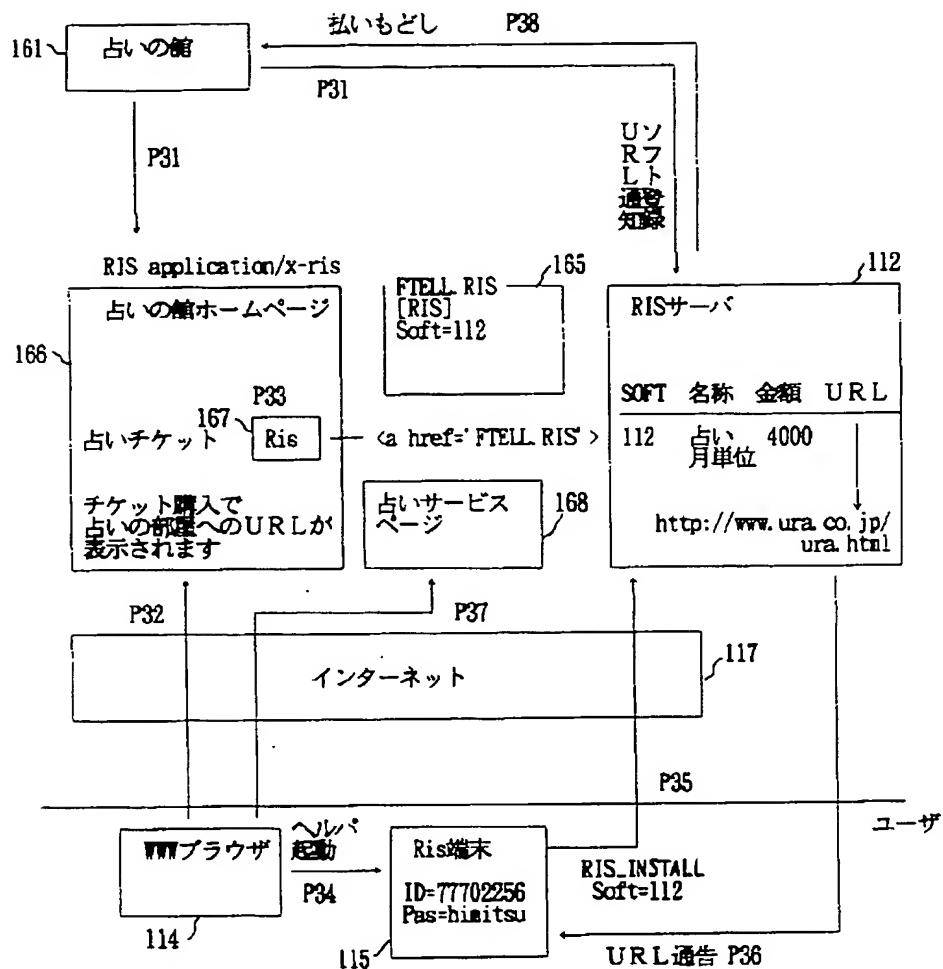


	D	E	F	G
FILE1.LZH	○	○	○	○
FILE2.LZH		○	○	○
FILE3.LZH			○	○



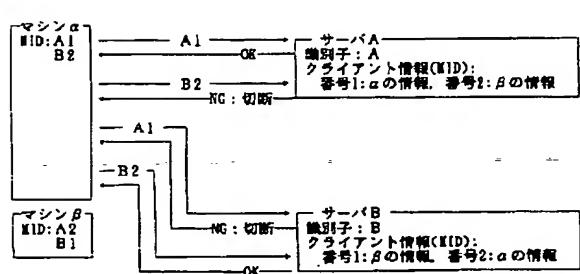
【図21】

## URLを通知する通信サービスシステムを示す図



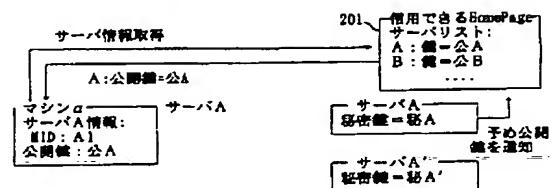
【図36】

## 複数のサーバが存在するシステムを示す図



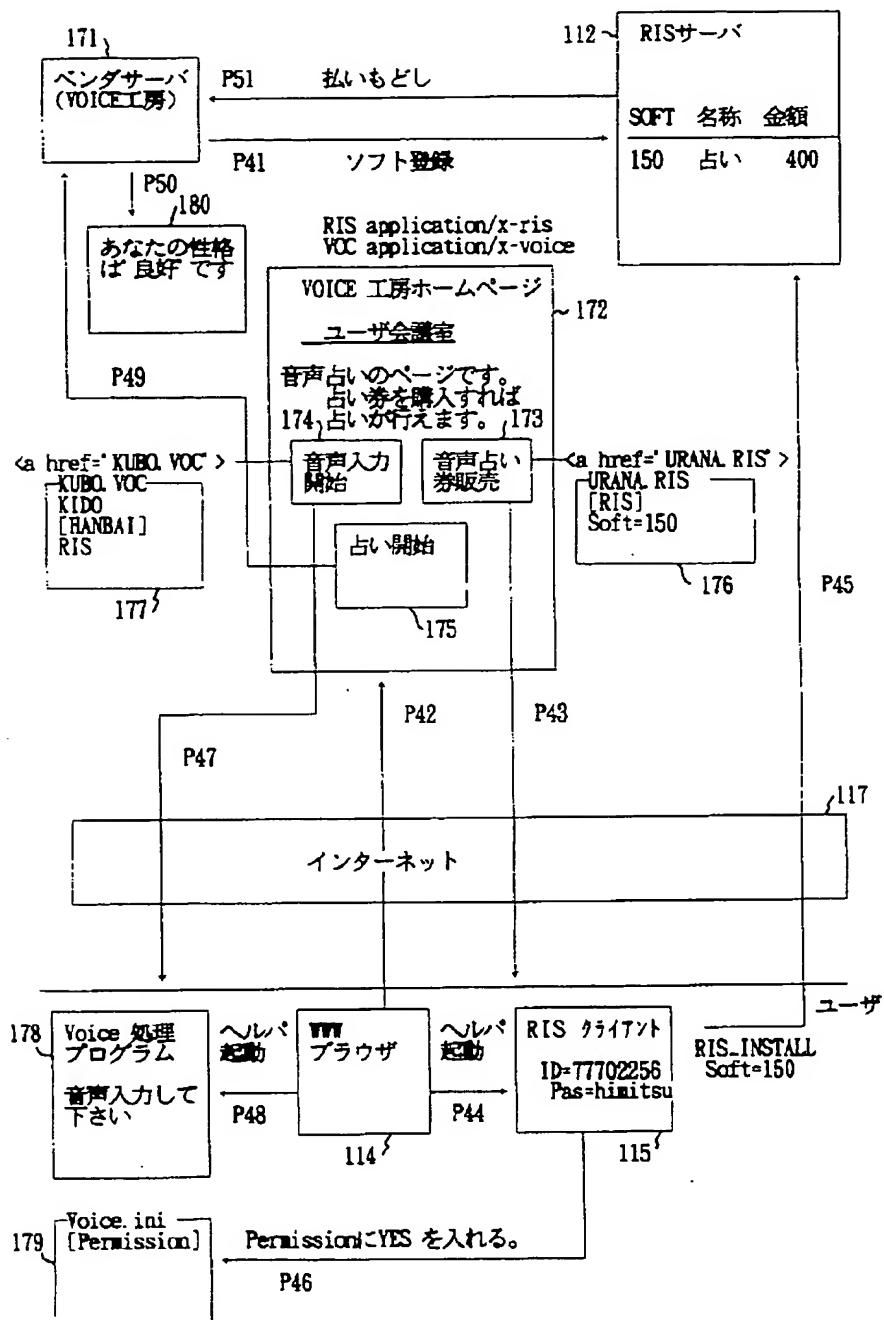
【図39】

## サーバ構成システムを示す図



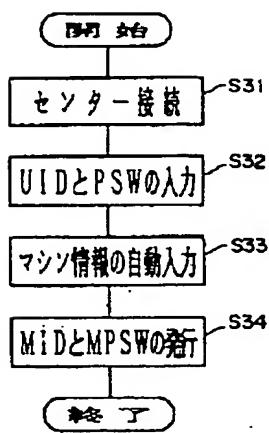
【図23】

## 第1のトランザクションサービスシステムを示す図



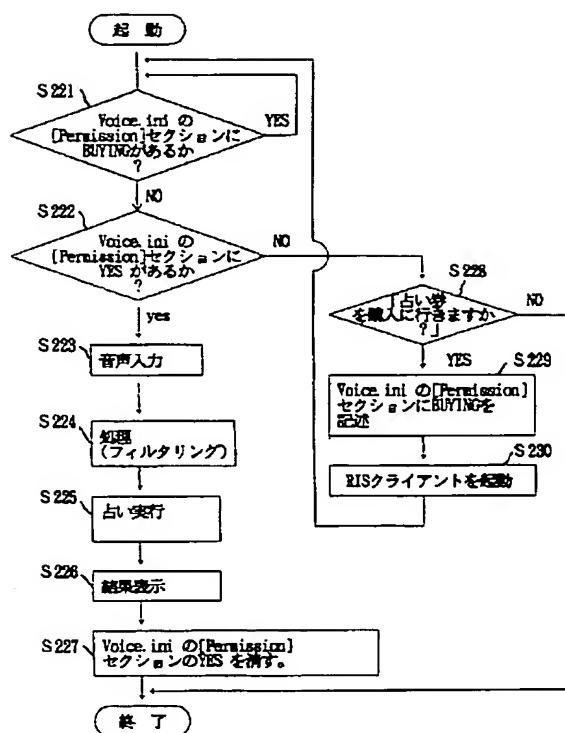
【図48】

## 端末ID登録のフローチャート



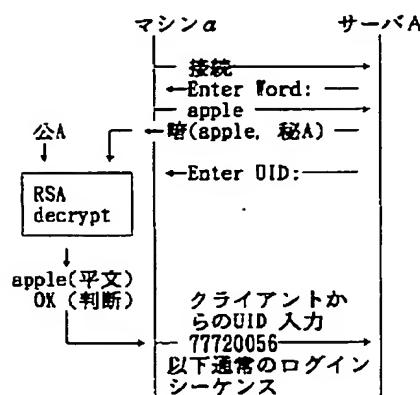
【図26】

## トランザクション処理プログラムのフローチャート



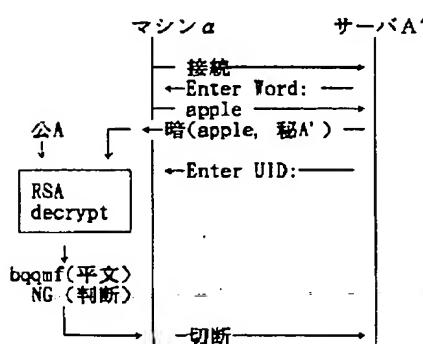
【図40】

## 第2のログインシーケンスを示す図



【図41】

## 第3のログインシーケンスを示す図



【図42】

## 第3のアンカーファイルを示す図

```

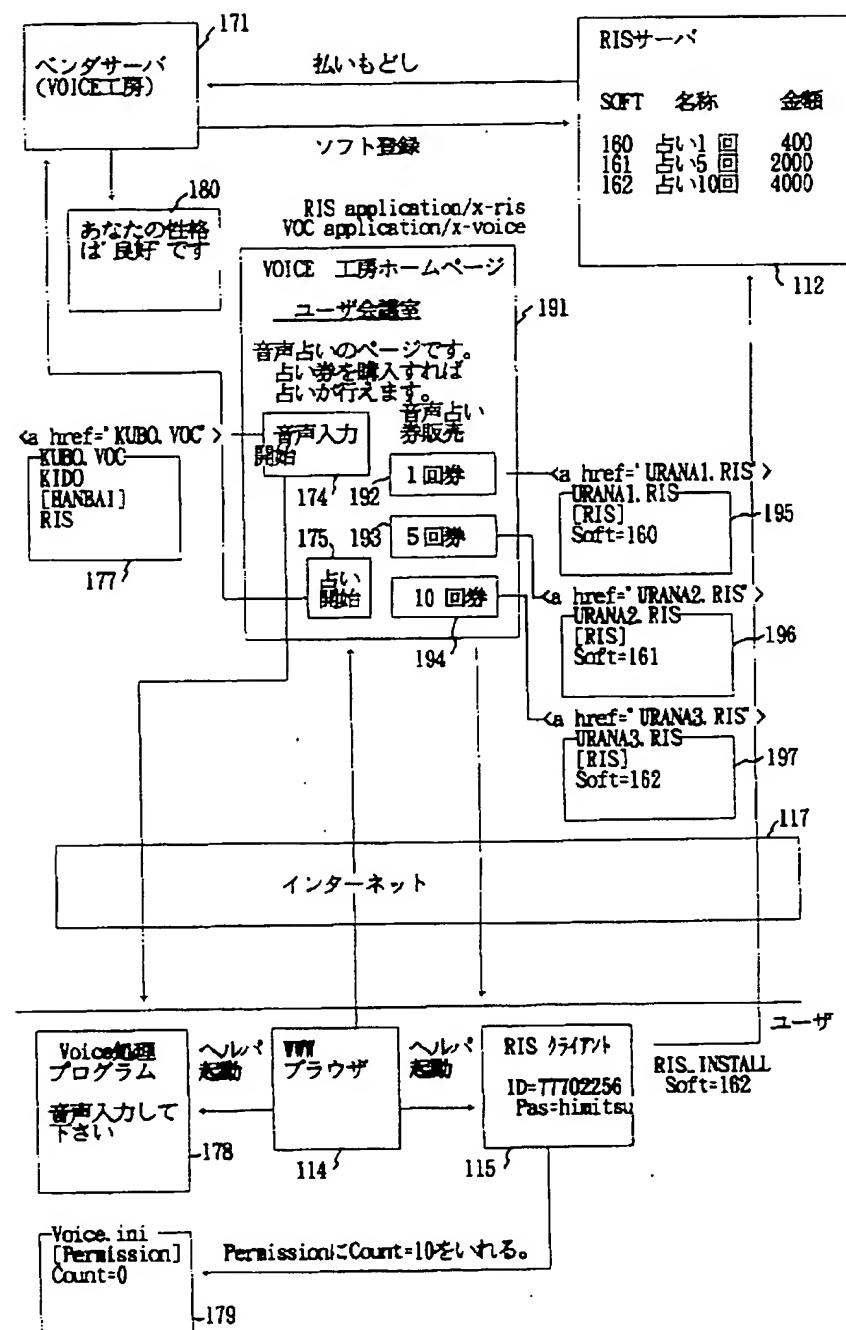
RIS2 RIS
[RIS]
Start-menu
[SERVER]
0002
[OKAY]
1234

```

This is a screenshot of an anchor file (アンカーファイル) showing configuration settings. It includes entries for RIS2, RIS, Start-menu, SERVER, and OKAY, along with their corresponding values.

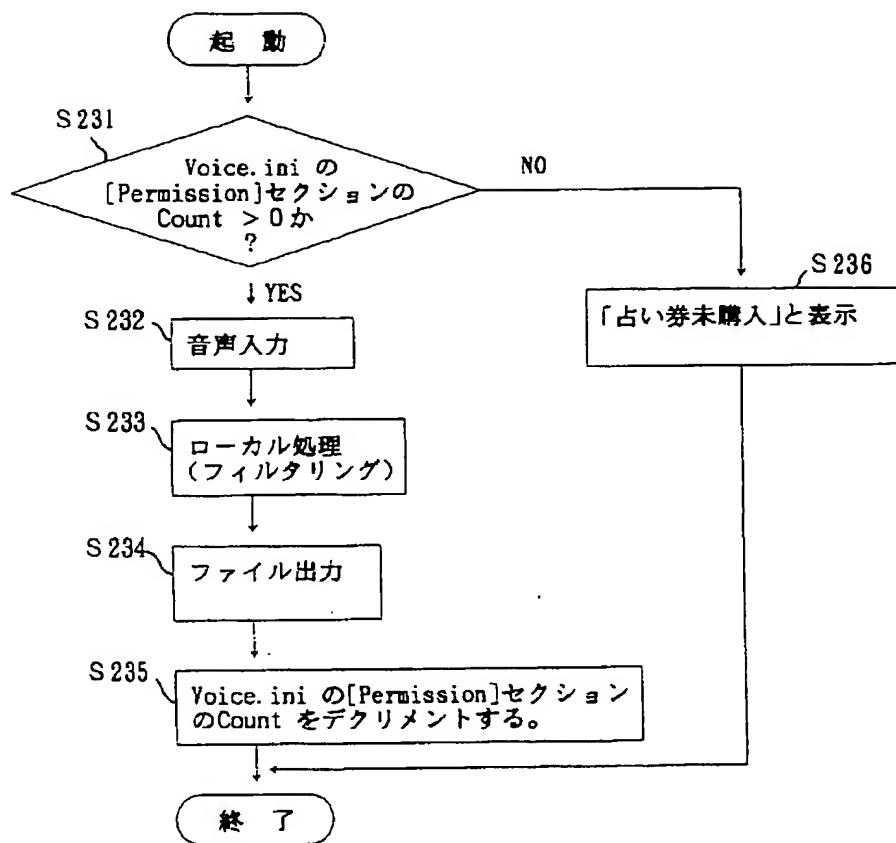
【図27】

## 第2のトランザクションサービスシステムを示す図



【図28】

## 第2のVoice処理プログラムのフローチャート



【図37】

## 第2の初期設定ファイルを示す図

```

RIS.INI
[SERVER]
0001
[INFO] ;*****
; SOUKODIR :倉庫ディレクトリ
; WORKDIR :ワークディレクトリ
; HOSTTEL :ホスト電話番号
; LSCRIPT :ポートオブ インクリプト(標準端末と同じ文法)
; COMPORT : COMポート ID
;
LSCRIPT=-^M[*]C RIS^M[COM]![Enter User-ID --->]$ID/P38/Y101^M[Enter
Password ->]SPT^M[Accepted/P38/Y101]
COMPORT=3
RISDIR=C:\RIS\418\RISWIN32
SOUKODIR=C:\RIS\418\VSOUKO
WORKDIR=C:\RIS\418\RISWORK
HOSTTEL=044-798-6500
INITFLAG=1
[IDENT] ;*****
; UID :ユーザ ID
; PASSWD :パスワード
;
TELAREA=044
→ UID=77702256
→ PASSWD=BAGFDE0FKP0B0EAFNB
KEY=S7FA40972F28A8A6B
[MACHINE] ;*****
; MODEL : モデル名
; OS : OS 名
; MID : マシン ID
; MTRANID : マシン ランダム ID

DS=2
→ MODEL=3
→ MID=537
→ MTRANID=001087127712
;MID=41
;MTRANID=000091397010

[INET]
InetPermission=Yes
HOST=ris.gsmnet.or.jp
PORT=5021
UsingINET=Yes

[EXTENSION]
RIS.INI=ON
RIS2.INI=ON
RIS3.INI=OFF

```

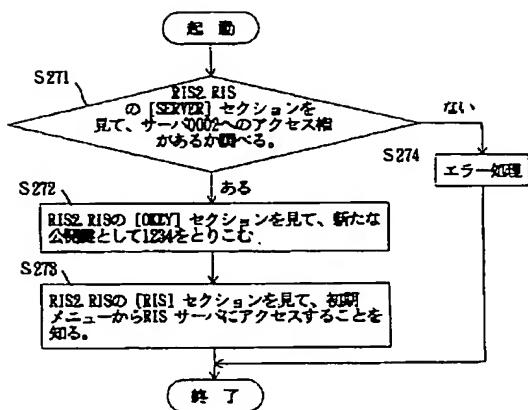
【図38】

## 第三の初期設定ファイルを示す図

```
RIS2.INI
[SERVER]
0002
[INFO] ;*****
; SOUKODIR : 金庫ディレクトリ
; WORKDIR : ワークディレクトリ
; HOSTTEL : ホスト 電話番号
; LSCRIPT : オート ログインスクリプト (標準端末と同じ文法)
; COMPORT : COMポート ID
;
LSCRIPT=^M[*]C RIS^M[COM]![Enter User-ID --->]SID/P98/V101^M[Enter
Password ->]SPW^M[Accepted/P98/V101]
COMPORT=3
RISDIR=C:\RIS\W418\VRISWIN32
SOUKODIR=C:\RIS\W418\VSOUKO
WORKDIR=C:\RIS\W418\VRISWORK
HOSTTEL=044-798-6501
INITFLAG=1
;
[IDENT] ;*****
; UID : 1-# ID
; PASSWD : パスワード
;
TELAREA=044
→ UID=11102256
→ PASSWD=BACFDE0FWHOEOEAFNB
KEY=S4FA40972F46A8A6B
;
[MACHINE] ;*****
; MODEL : モデルコード
; OS : OS コード
; MID : マシン ID
; MTRANID : マシン トランザクション ID
;
DS=2
MODEL=3
→ MID=637
MTRANID=002087127712
[INET]
InetPermission=Yes
HOST=ris2.gmsnet.or.jp
PORT=5021
UsingINET=Yes
```

【図43】

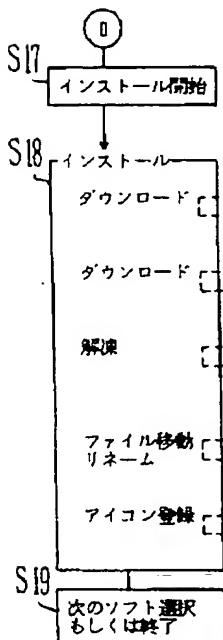
## クライアントの処理のフローチャート



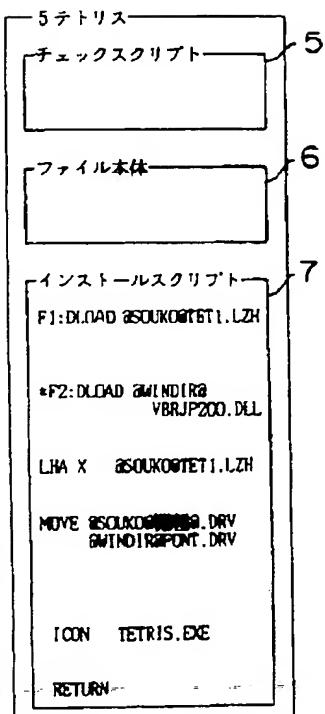
【図46】

## リモートインストールのフローチャート(その3)

クライアント側

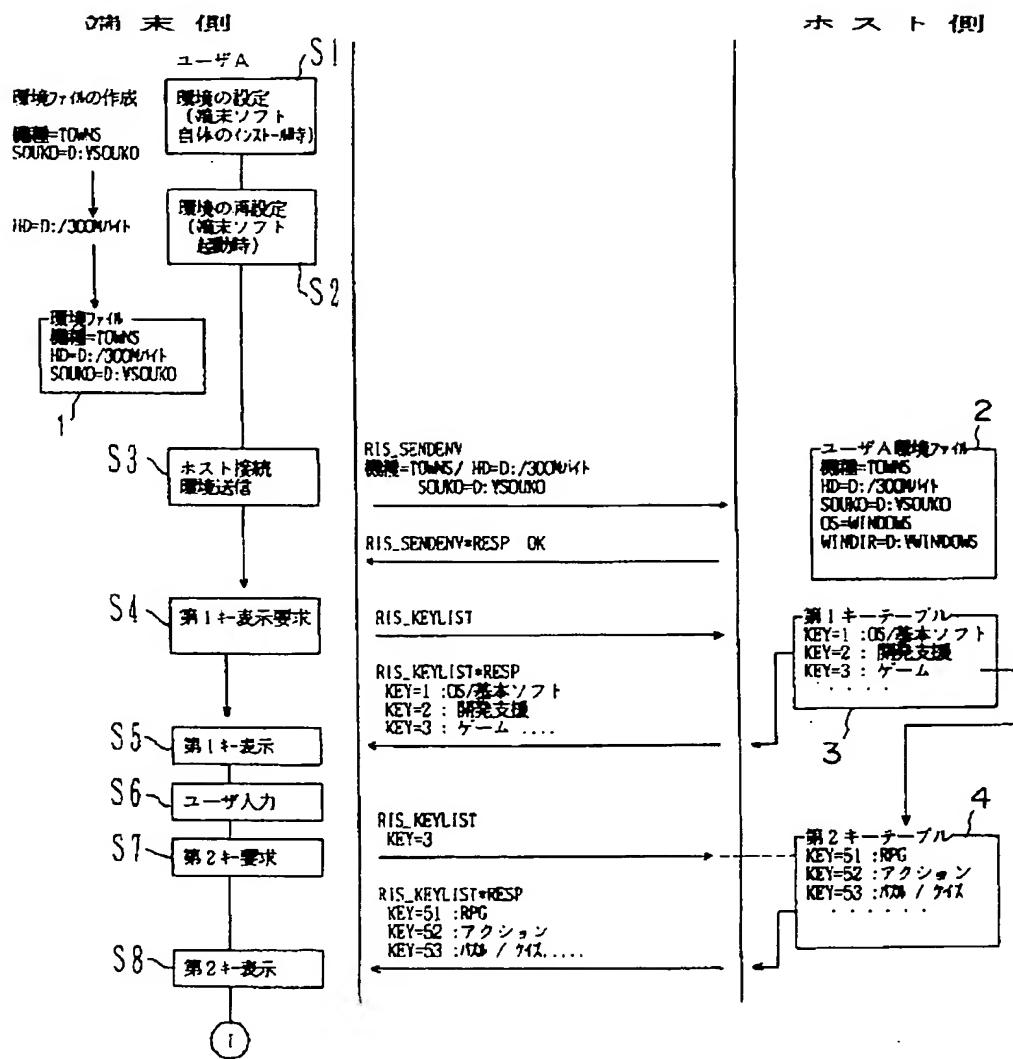


ホスト側



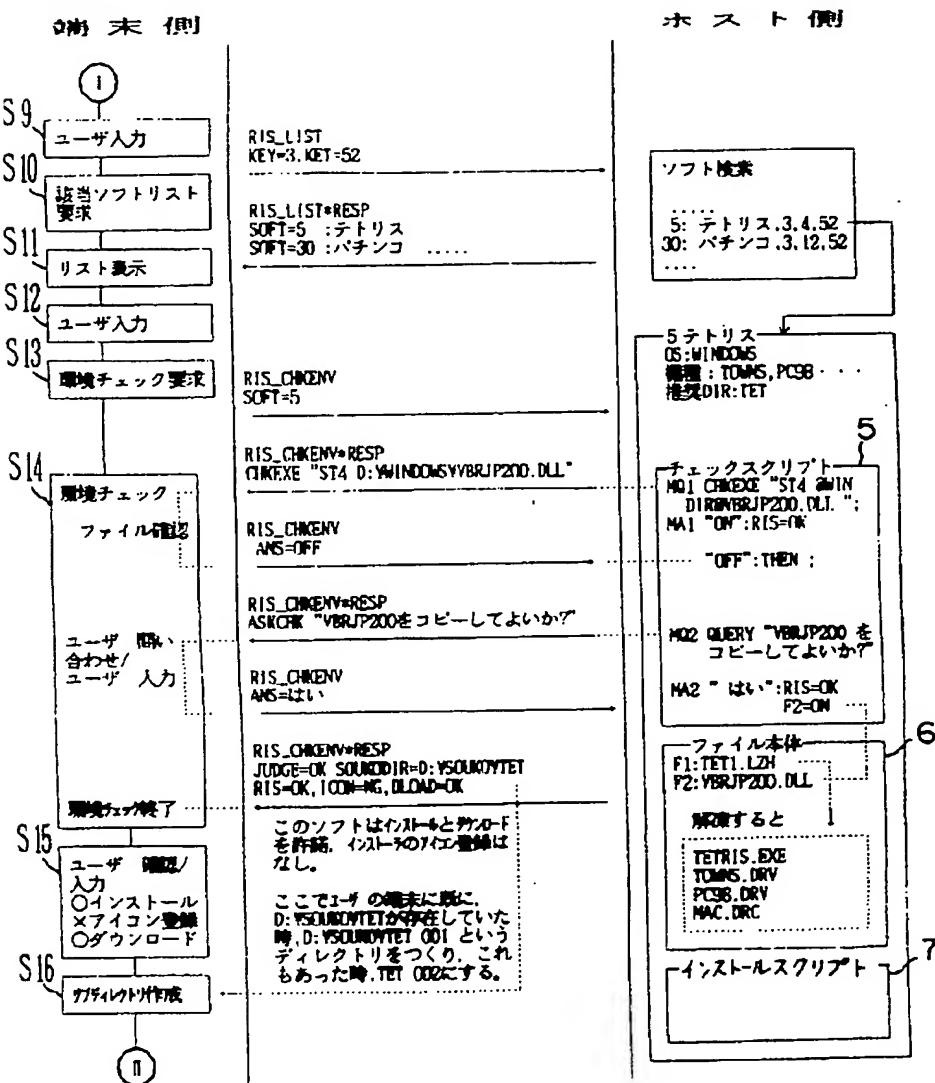
[図44]

## リモートインストールのフローチャート(その1)



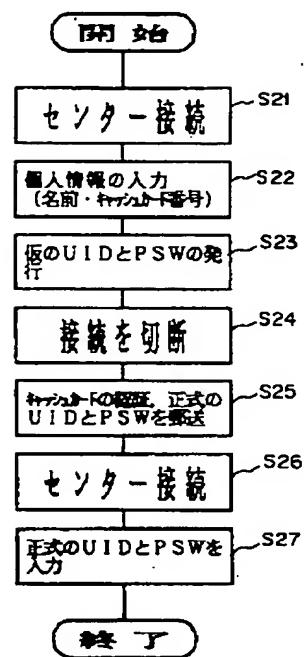
【図45】

## リモートインストールのフローチャート(その2)



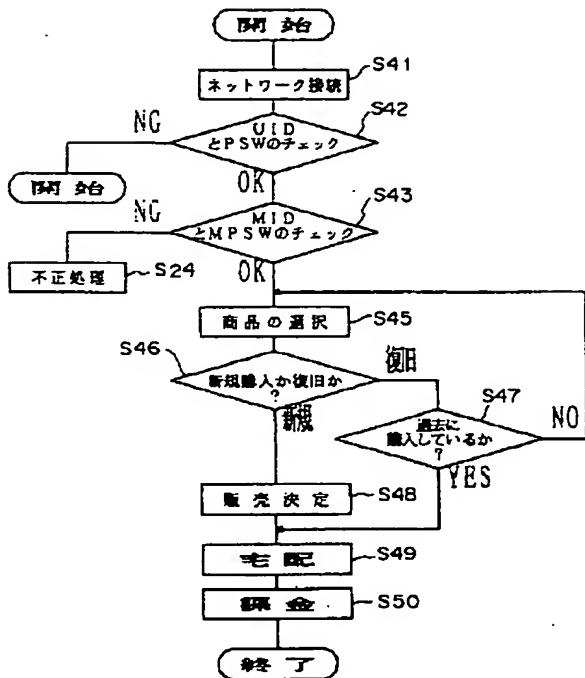
【図47】

## ユーザID登録のフローチャート



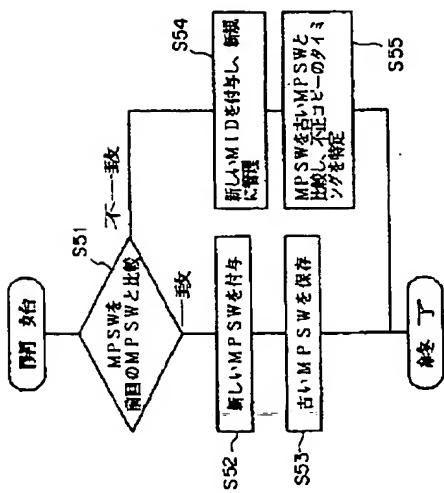
【図49】

## 販売のフローチャート



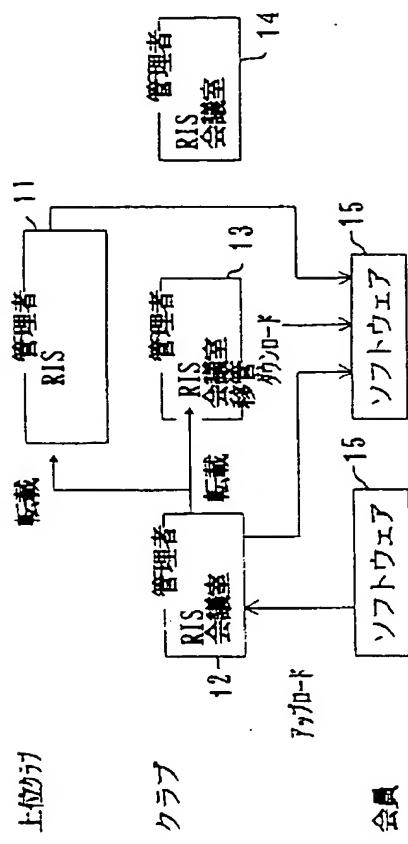
【図50】

## 端末パスワードチェックのフローチャート



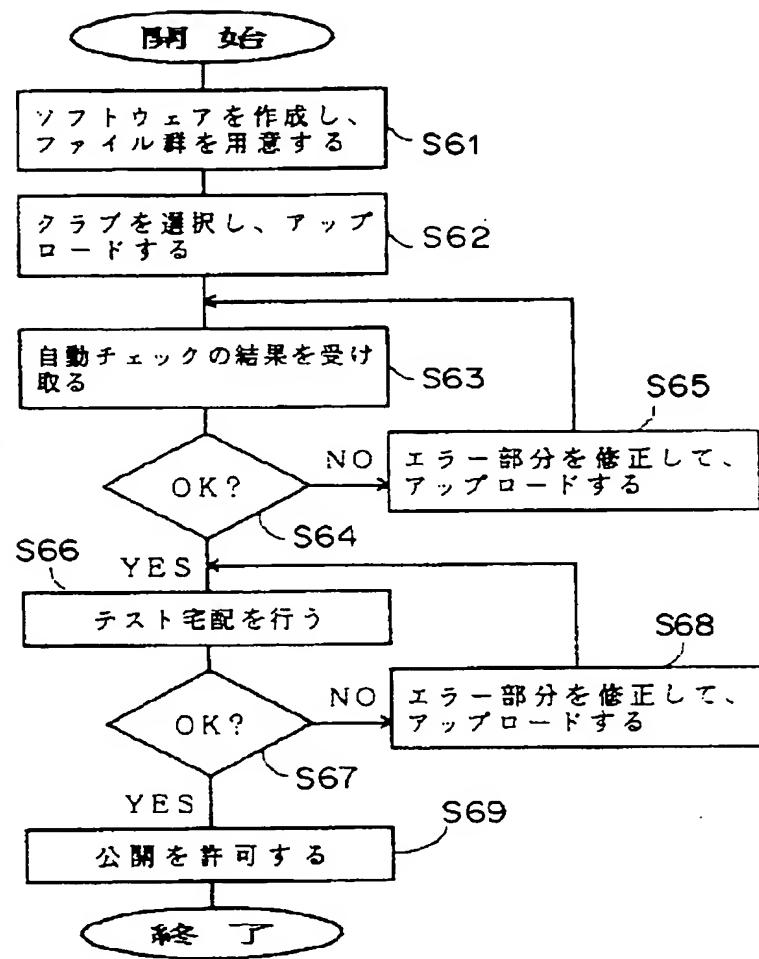
【図51】

場の構成を示す図



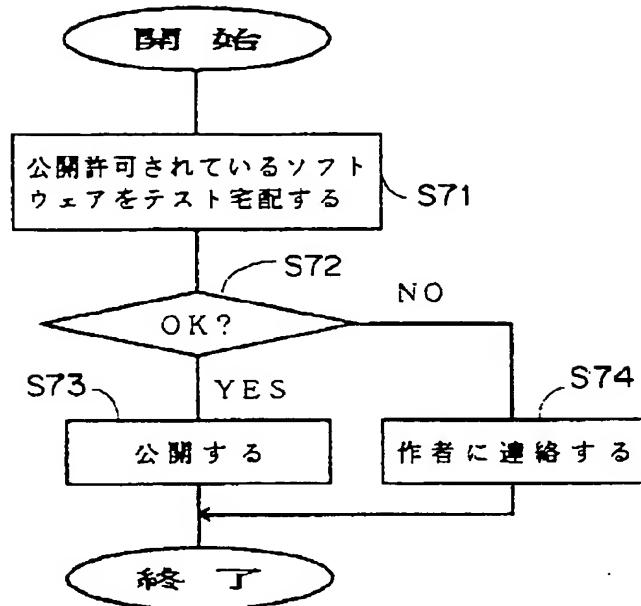
【図52】

作者の作業のフローチャート



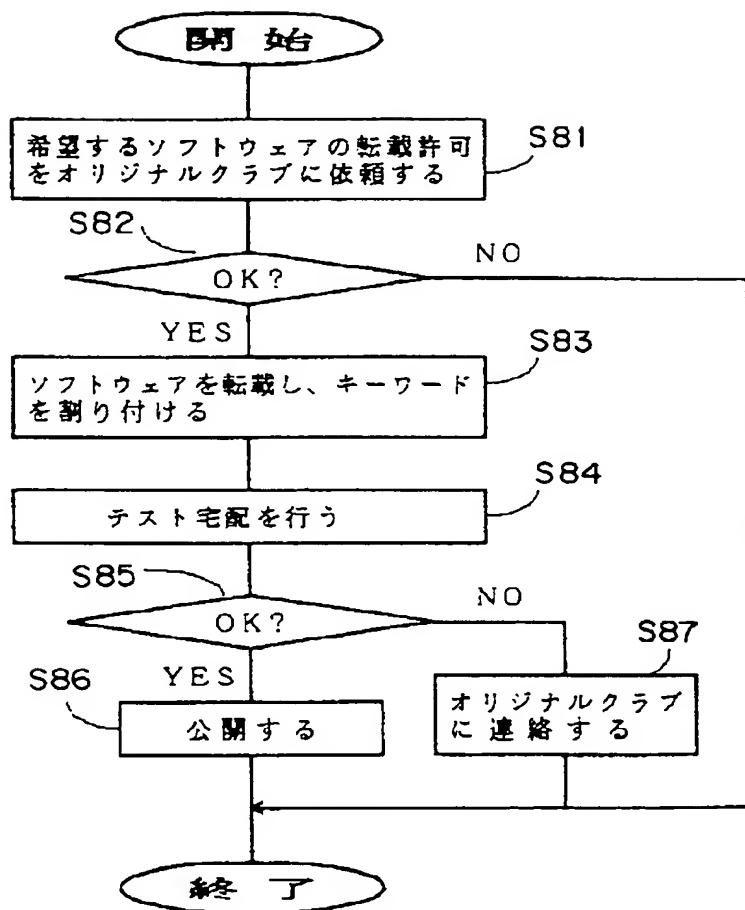
【図53】

## オリジナルクラブ管理者の作業のフローチャート



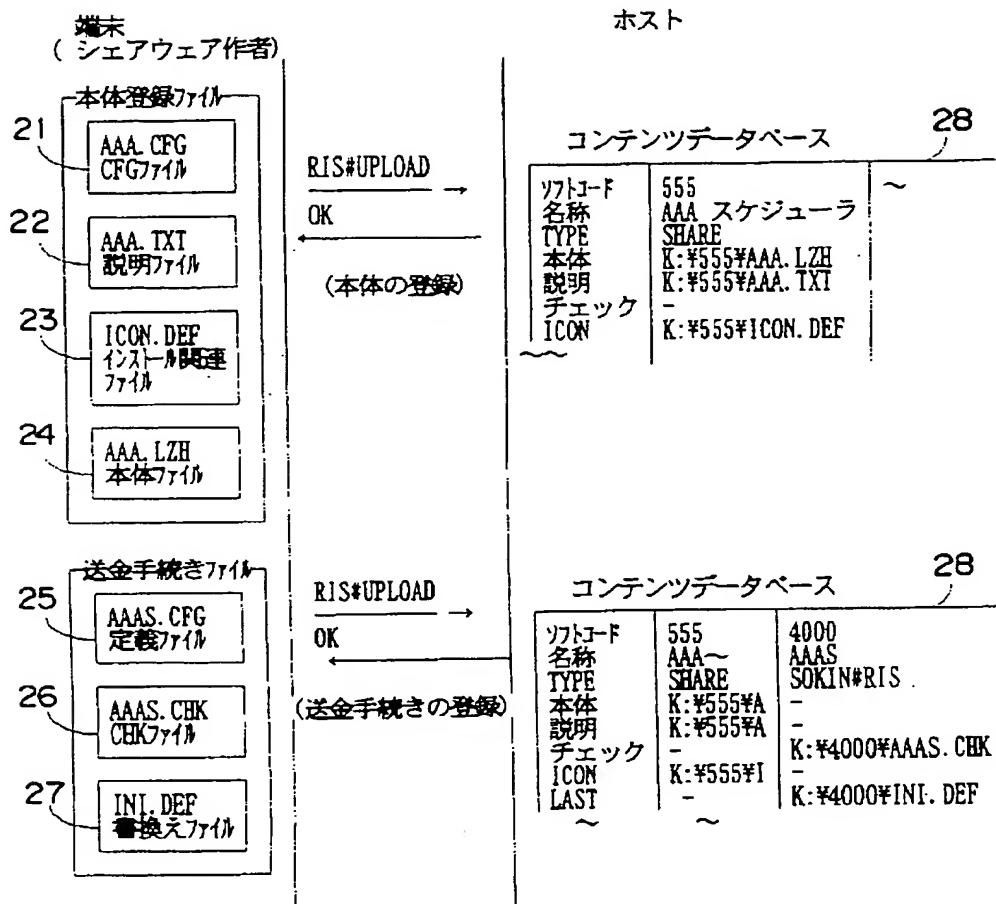
【図54】

## 転載先クラブ管理者の作業のフロー・チャート



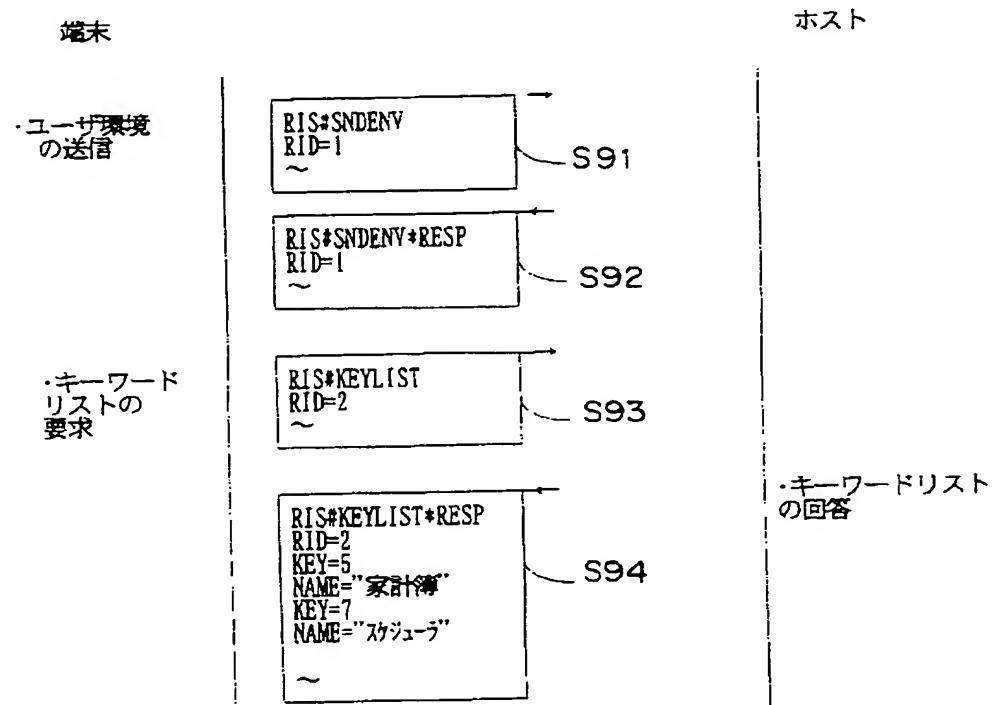
【図55】

## アップロードを示す図



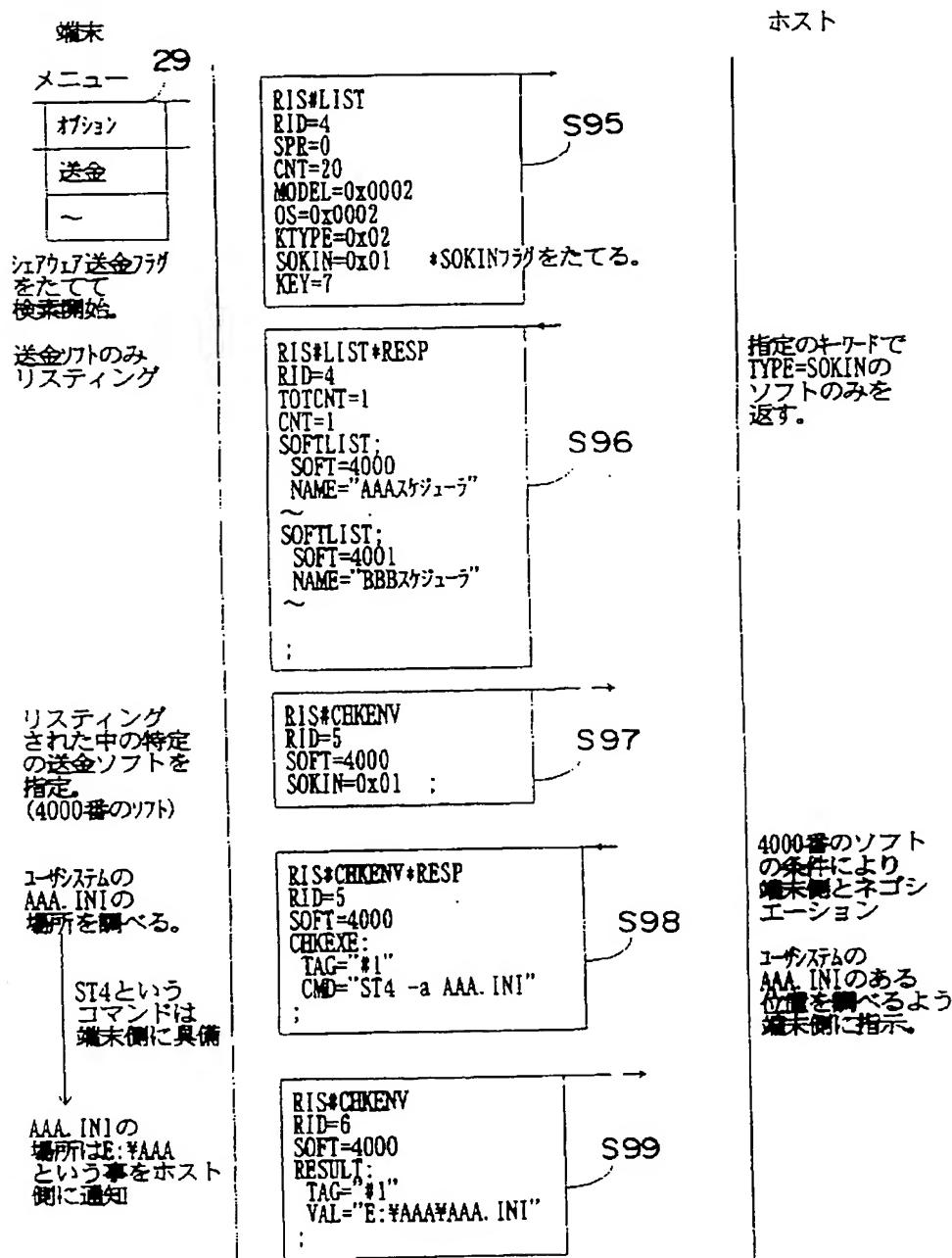
[図56]

## シェアウェア手続きを示す図（その1）



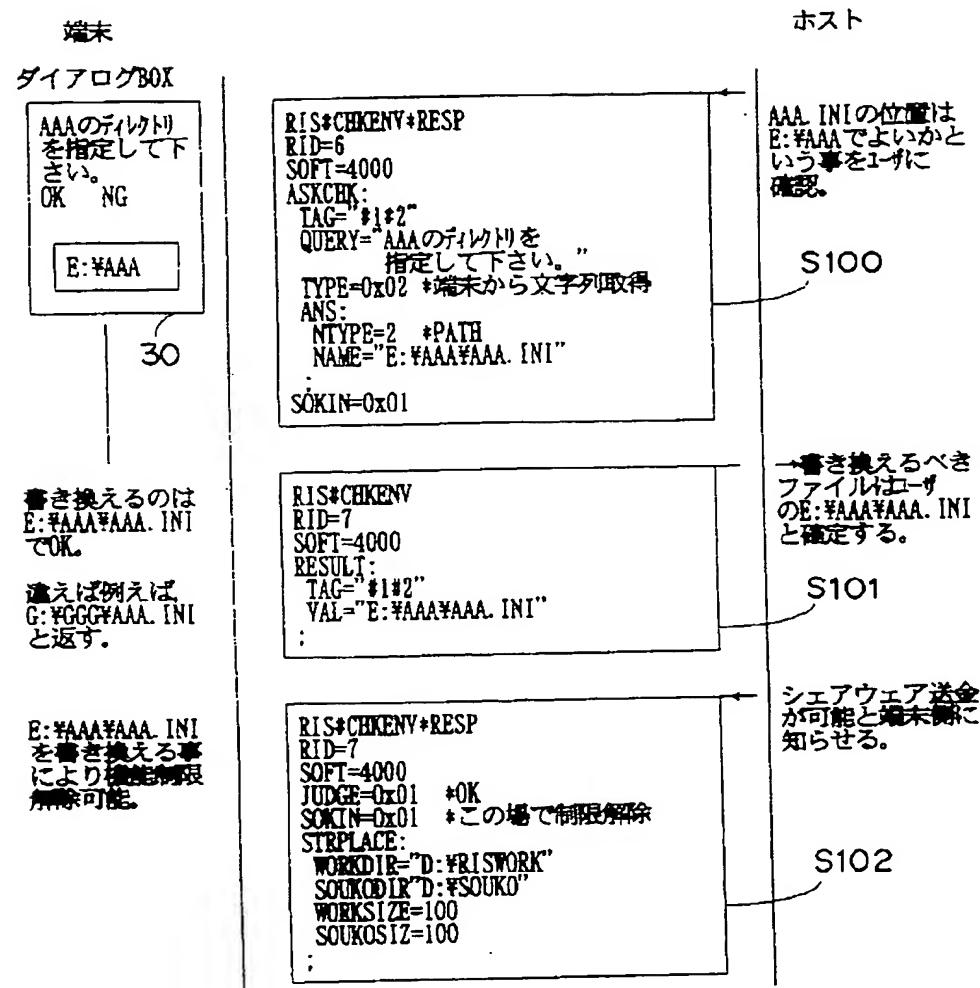
【図57】

## シェアウェア手続きを示す図（その2）



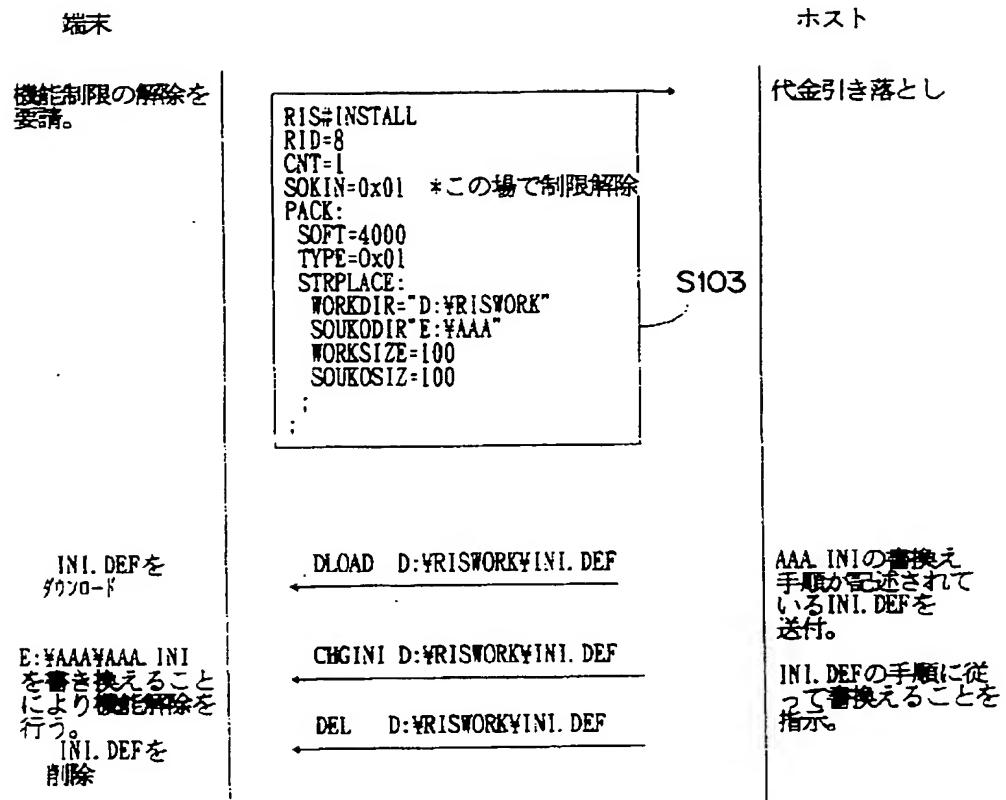
【図58】

## シェアウェア手続きを示す図（その3）



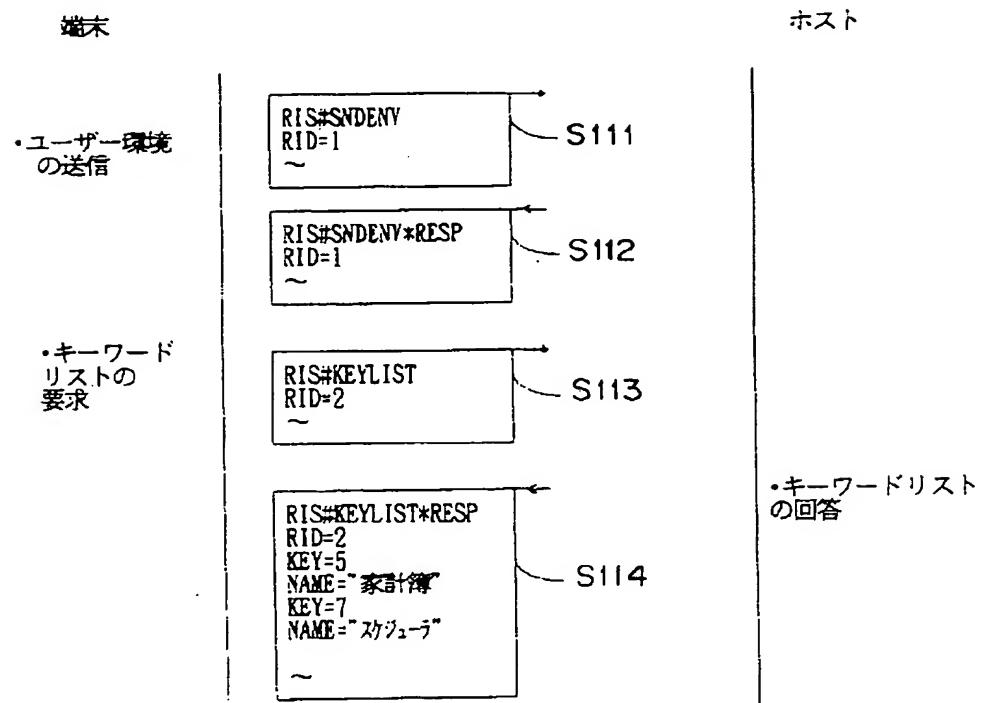
【図59】

## シェアウェア手続きを示す図（その4）



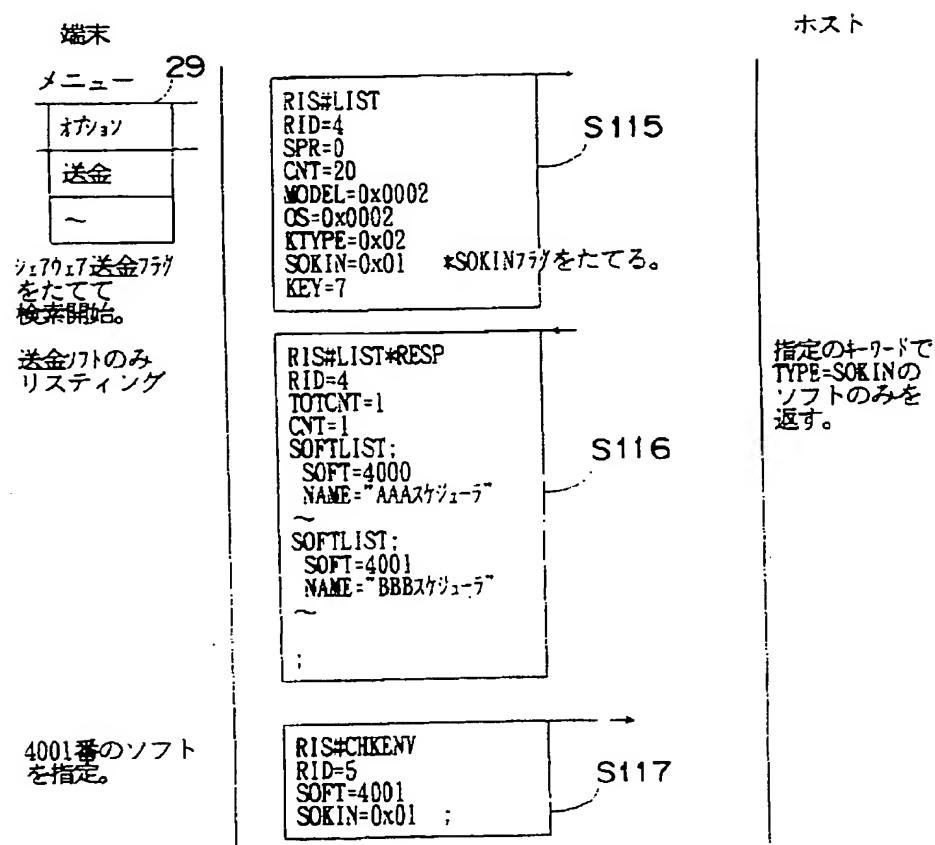
【図60】

## 代金引き落とし手続きを示す図（その1）



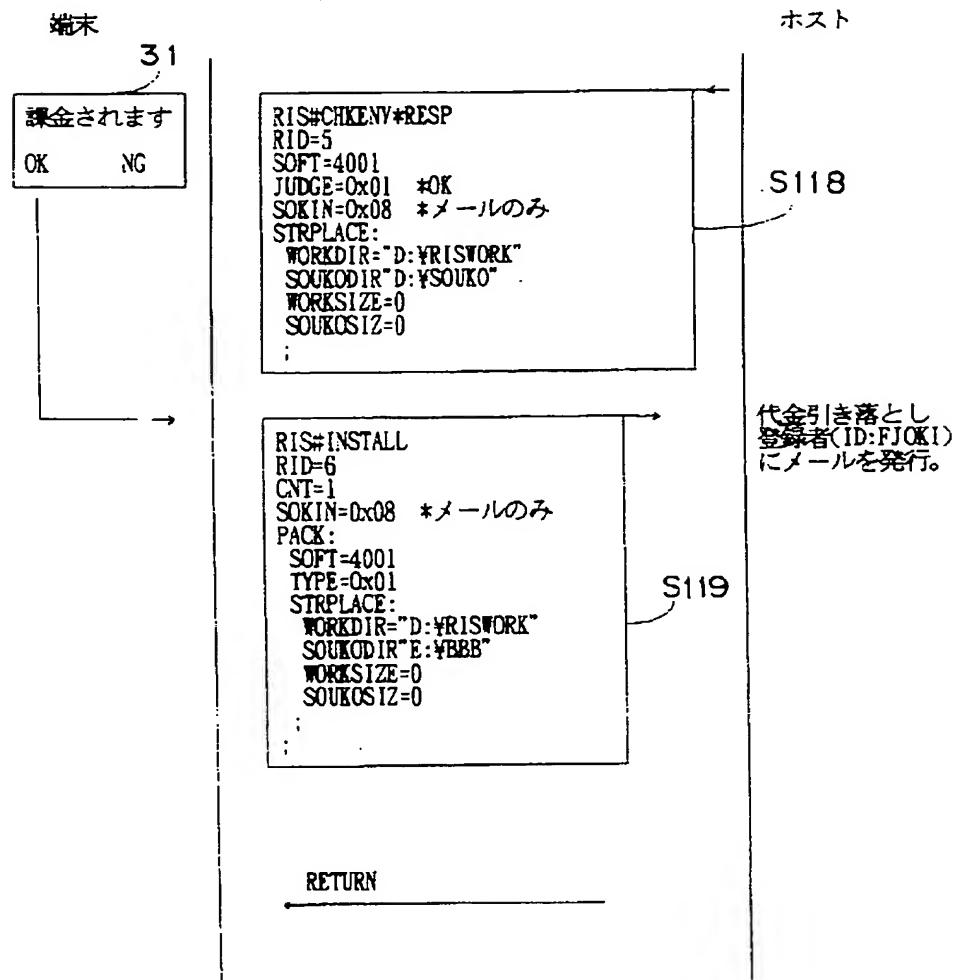
【図61】

## 代金引き落とし手続きを示す図（その2）



【図62】

## 代金引き落とし手続きを示す図（その3）



フロントページの続き

(72) 発明者 中村 直人  
 神奈川県川崎市中原区上小田中4丁目1番  
 1号 富士通株式会社内

(72) 発明者 山㟢 利哉  
 神奈川県川崎市中原区上小田中4丁目1番  
 1号 富士通株式会社内  
 (72) 発明者 岡田 利司郎  
 神奈川県川崎市中原区上小田中4丁目1番  
 1号 富士通株式会社内